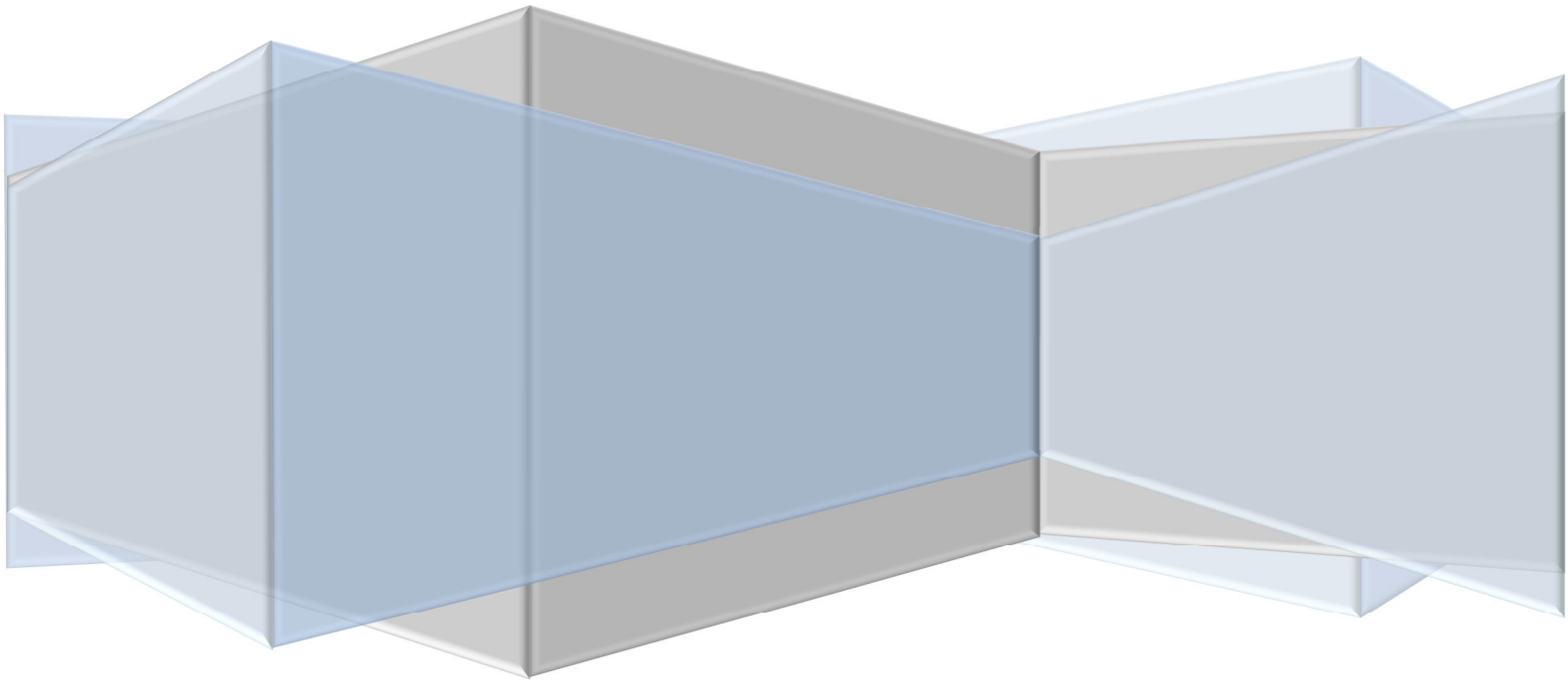
November, 2010

Briefing on the internet, e-commerce, children and young people

Children's Charities' Coalition on Internet Safety



children's charities' coalition on internet safety

Briefing on the internet, e-commerce, children and young people

The Children's Charities' Coalition on Internet Safety (CHIS) has recently responded to three different consultations which in one way or another touch on the position of children and young people as internet users in the context of e-commerce. One was organized by the UK's Ministry of Justice, one by the Office of Fair Trading and one by the Commission of the European Union.

The new document here presented is a consolidated version of our responses to all three consultations. It also updates aspects of the original three and has benefited from comments made on them since one or other was first published.

The charities within CHIS share a common determination to ensure that all children and young people everywhere have an equal opportunity to enjoy safe access to the internet in order to benefit from the many advantages it provides across a broad spectrum of social, educational, commercial and cultural activities.

The huge expansion of the internet, and in particular the major growth in online commerce in recent years, especially the shift to online retailing, has created several new challenges in terms of child welfare and child protection. It is evident that many of the traditional safeguards against the commercial exploitation of children and young people, painstakingly developed over many years in the real world, have yet to be fully translated into the virtual world or to find an equivalent or proxy.

CHIS would like to record its thanks to Professor Agnes Nairn of the EMLyon Business School for her invaluable advice and comments when preparing this paper although CHIS alone is responsible for the final contents.

John Carr OBE
Secretary
CHIS
The Boulevard
Ascot Road
Watford
WD18 8AG
www.chis.org.uk

November, 2010.

Contents

Executive Summary

Policy challenges

1. Children and young people constitute a significant target market for many different types of businesses. They are major economic actors, both in their own right and in terms of influence exerted on expenditure within the wider family.

2. Several of the rules and practices which have been established to protect children and young people from unfair commercial practices in the real world do not yet seem to have been fully translated into the virtual space or to have found an online equivalent or proxy.

Data collection and online advertising

3. In both the offline and the online worlds data collection should be based on the informed consent of the individuals concerned.

4. There are continuing suspicions that many online companies are failing to discharge properly their obligations to obtain informed consent from adults who use their services. This raises grave doubts that they are doing so at all satisfactorily in relation to children and young people where the burden is heavier.

5. A computer screen is not a natural or easy medium for grappling with lengthy and sometimes highly technical legal language. The screen of a typical mobile device is even less suited to this task.

6. The complexity of multiple control settings, frequently located in obscure parts of the site, spread across different sections or buried within applications, rarely helps children or young people or their parents to understand the nature of the proposition. Bamboozled or fatigued consumers are unlikely to be properly engaged or informed.

7. High Street firms that fastidiously observe the established principles of data collection and data usage in relation to minors are seeing their position unfairly undermined by online companies that collect data on, from or via web sites that are either indifferent to or incapable of reliably determining the age of their customers, users or visitors.

8. Far from having an incentive to discover the true ages of their customers, users or visitors, many web sites have a material interest in not knowing the real ages.

9. The foregoing observations are particularly true in relation to the so-called “free internet” i.e. online services provided at no cost at the point of use, financed largely through advertising.

10. The use of the term “free internet” is in any event deceptive. It simply describes a different business model i.e. a model which uses alternative ways of generating revenues, typically advertising.

11. It is acknowledged that a degree of latitude should be allowed to sites which provide services free at the point of use, but there ought to be a discussion about its limits.

12. Many online companies claim not to target children and young people with advertising but there is some evidence to suggest it may be happening anyway, whether intentionally or not. The emergence of a new breed of internet based location aware applications and services is likely to generate new anxieties in this regard.

Age restricted goods and services

13. The online sale of age restricted goods and services is a singular example of how laws created for an analogue world have, with limited exceptions, hitherto proved to be largely ineffective in the digital world. Here, paradoxically, it is the deliberate and continuing failure of companies to collect accurate and sufficient data that is putting children and young people at risk.

14. Following sustained efforts by trading standards officers, High Street shops are consistently found to have a high rate of compliance with the age related laws e.g. in relation to the sale of alcohol, knives and tobacco. The opposite is true with their online counterparts. This unfairly undermines the viability of companies trading principally on the High Street.

Sustainable confidence and trust

15. To build sustainable trust in the internet, inter alia, it is important to address the tensions, anomalies and misalignments in policy which have been created by the emergence of the internet as a major force in online commerce, particularly in retailing.

16. Market distortions and unfair competitive practices have developed, some of which are closely connected to online risks to children and young people both in terms of commercial exploitation but also in ways which spill over into other dangers to children's and young people's health and welfare.

Policy proposals

17. As part of the backdrop to further policy development research should be commissioned into the full spectrum of vulnerable internet users, giving particular attention to children's and young people's engagement with the commercial aspects of the internet.

18. The Government should bring together or initiate a discussion with all of the relevant stakeholders and regulators with an interest in online commerce and its associated practices to focus specifically on the position of children and young people in relation to online commerce. The UK Council for Child Internet Safety could play an important part in drawing together the different strands.

19. Consideration should be given to requiring all companies to perform a "child safety audit" prior to the release of any new product or service on to the internet, particularly, though not exclusively, if it is going to be made available on the "free internet". An appropriate agency should have the power to call in and inspect the audits either on their own volition or following a complaint.

20. The fact that children and young people are economic actors and targets on the internet ought to be explicitly recognized and incorporated into future policy making, both generally but also specifically in relation to policy around tracking technologies and the advertising and data collection practices which they facilitate.

21. Acknowledging that children and young people are major economic actors targeted online by commercial concerns, media literacy initiatives need to be encouraged which should, inter alia, focus on this dimension to the internet, underlining the key role of data collection and advertising.

22. A definition and method of determining what constitutes a children's web site or other area of online activity may need to be agreed. Specific rules governing advertising and data collection on or from such locations may need to be developed. For example, should children's and young people's web sites, or sites used by large numbers of children and young people, be encouraged to develop a system of easily understood icons to indicate, explain and overlay the site's fuller data collection and data usage polices?

23. The position in UK law, which seems to require companies to carry out a subjective assessment of each child's comprehension of every proposed data transaction, as a prelude to determining whether or not they might lawfully engage with the child, is a counsel of perfection which is unlikely to be workable in the online world in the foreseeable future, or indeed ever. It may be better to follow the example of Spain and the USA and prescribe a definite lower age limit which would apply *solely* in the context of the internet or other remote environments. Could such an age limit be translated into a generic online safety threshold?

24. The fact that the gambling industry has been able to introduce successfully a system which keeps children off their sites proves that, at least so far as the sale of products and services rated 18 and above are concerned, scalable working solutions are available now. They are simply not being taken up. They should be.

25. Consideration should be given to establishing a licensing system similar to that which exists within the gambling industry i.e. in order to sell any age restricted product or service online a licence would be required and these will only be issued if the vendor could show they had put in place a robust age verification system which works at the point of sale.

26. A licensing system which works in respect of goods and services which have 18 as their minimum age could be established relatively easily and quickly because the technology and accessible online databases already exist. It is acknowledged that devising systems to ensure compliance with laws and regulations affecting the sale of goods and services which are restricted to persons under the age of 18 e.g. certain computer games and films, requires more focused attention to devise scalable

solutions. What has been lacking is any obvious determination on the part of major online retailers or the financial institutions, or both, to resolve the problem of how to originate, authenticate and keep secure the primary or initial data. Each sector seems to think it is the other's responsibility. In reality they have a shared responsibility. The Government should consider pressing for a joint initiative to take this forward within an acceptable timeframe.

27. Real world checks made at the point of delivery can never be a complete alternative to online age verification at the point of sale. Whilst not opposed to the idea of making age related checks at the point of delivery, and in some cases perhaps for certain items this should be required, as a general proposition their practicality is very dubious. The most obvious area where this would not work concerns items which are paid for online and wholly consumed online.

Introduction

Definition of a child

In this document, except where the context provides otherwise, a child or young person is defined as someone who has not yet reached the age of 18[1].

This does not mean CHIS takes the view that a typical child of three or four should in all respects and in every circumstance be treated the same way as a typical young person of 16 or 17. However, the principal focus of this submission is children and young people as economic actors. For most purposes in commerce 18 is a key point of departure.

The general law

In England, Wales and Northern Ireland a person acquires full contractual status at 18. In Scotland young people acquire elements of full contractual status at 16[2].

In England, Wales and Northern Ireland below the age of 18 a young person may only form an enforceable contract for items which are considered “necessities”.

It is acknowledged that what constitutes a “necessity” can change over time but none of the products or services which are discussed here could fall within any reasonable definition of that term. For practical purposes the law in Scotland operates in a similar way.

Whilst the general rule for adults in relation to the law of contract is “buyer beware” where minors are concerned the vendor can be held to a higher standard.

Chapter 1
Policy overview

Public policy

It has been the policy of successive UK Governments to encourage widespread take up of the internet.

It now seems commonly accepted that higher levels of internet usage produce direct benefits to the economy[3]. To the extent that more use is made of the internet to order goods which are delivered by multi-drop off vans, it also produces environmental and other advantages.

Children and young people, defined for these purposes as persons between the ages of 4 and 17, constitute a very large and persistent group of internet users within the UK, as indeed they do throughout the EU27[4] and further afield.

Schools, both public and private, have been key to establishing the large scale take up of the internet among children and young people. Teaching has undergone a series of radical changes to make greater use of the richer learning environments that the internet can provide.

Children and young people without convenient internet access at home are now acknowledged to be both at a social and at an educational disadvantage[5]. For that reason the last Government promoted a scheme, the "Home Access Initiative"[6], aimed at ensuring every child of school age in England[7] had a computer and an internet connection at home, irrespective of their parents' ability to pay. The new Government has said it will preserve elements of the scheme.[8]

Whilst "Home Access" was primarily grounded in educational policy[9], the appeal to parents was based in part on the economic and other advantages that being online brought to the whole family. Being online is good for Britain is the strong public policy message from all quarters.

Children and young people online

Children and young people arguably make up the largest single vulnerable group within the UK[10], both generally and also in relation to the total number of internet users. It is traditionally expected that extra steps are taken to ensure children and young people, or other vulnerable groups, are properly safeguarded from risks or situations which a fully competent adult would normally know how to handle. In much online commerce, in practice, sadly such extra steps appear to be the exception rather than the rule.

As part of the backdrop to further policy development research should be commissioned into the full spectrum of vulnerable internet users, giving particular attention to children's and young people's engagement with the commercial aspects of the internet.

No stereotyping please

In any discussion about children, young people and the internet it is very important not to fall prey to stereotyping or misplaced assumptions. It is true that a great many children and young people have been eager, easy and early adopters of the new technologies, but not all have been. This really should not be a surprise. Not all children and young people are the same. They will not all experience the internet in an identical way. They will not all always feel equally comfortable around

any and every new technology[11]. Yet society has an obligation to all children, not just some, and companies have obligations to all of their customers, not just the majority.

In her pioneering work LSE's Professor Sonia Livingstone showed, inter alia, the popular idea that every child and young person was ranging far and wide on the internet, exploring every virtual nook and cranny is a myth. On the contrary Livingstone found

> **The internet is not yet used to its full potential**.
>
> Many children and young people are not yet taking up the full potential of the internet, for example visiting a narrow range of sites or not interacting with sites.

Perhaps of particular importance in the context of e commerce, in the same study Livingstone also found

> **Children lack key skills in evaluating online content:**
>
> 38% of pupils aged 9-19 trust most of the information on the internet, and only 33% of 9-19 year olds daily and weekly users have been taught how to judge the reliability of online information.[12]

Livingstone's observations underline the importance of improving children's and young people's media literacy both generally but also specifically in relation to online commerce, including the role played by data collection.

The importance of age

The emergence of the internet as a major force in online commerce, particularly in retailing, has produced a number of new challenges. In relation to children and young people, these challenges turn principally on how companies approach the question of age.

The issues come most sharply into focus in relation to the sale over the internet of age restricted goods and services and in relation to the collection and use of data containing personally identifiable information which is provided to or used by advertisers. The latter applies particularly in relation to the so-called "free internet" but also more widely.

A new perspective on the internet

In 2010 the internet has become many different things to many different people but part of it is unquestionably a consumer commodity. Internet connectivity packages are often sold as part of a deal linked to offerings from domestic cable TV or telephone companies. "Toys R Us" sells wireless routers and laptops. It is therefore important to stop thinking about the internet as if it were, essentially, still primarily an adult or business medium for which special (often meaning "irritating") provisions need to be made to take account of the fact that children and young people will use it occasionally for homework or some other "fleeting or trifling" purpose.

Children's and young people's substantial and constant engagement online has to become central to thinking about how policy evolves across the whole space.

Addressing online child protection and related issues requires the involvement of many stakeholders: Governments, schools, industry, law enforcement, NGOs, parents and of course children and young people themselves. No one group or sectional interest can do it all on their own. No one is exempt.

Many people have been heard to say that there would be no problem at all with children's and young people's use of the internet if only parents supervised them properly. CHIS is very much in favour of

encouraging greater parental involvement in all aspects of their children's lives and upbringing, but the fact that this might sometimes breakdown does not mean that, for example, online retailers are therefore freed of any obligation to obey the law. If a child turns up in a supermarket and asks for a bottle of whisky this does not give the company permission to hand it over. It should be exactly the same in cyberspace.

The internet is now more akin to a modern city. In the modern city there are planning, zoning and other laws to govern who can do what, and where and when they can do it. Much more effort needs to be put into developing cyber equivalents. The internet needs to be embraced wholeheartedly as a social place, populated and used by many different interests of which families with children are one, and not the least one.

It is very dispiriting to hear internet company executives and Government officials repeating the mantra about how what is legal in the real world is legal in the online world, and what is illegal in one is equally illegal in the other when so very obviously the rhetoric is such a long way from matching the reality.

Tensions, anomalies and misalignments

CHIS argues in this paper that the arrival of the internet as a major force in online retailing has created a number of glaring tensions, anomalies and misalignments in policy. In earlier times these did not exist at all or they mattered a great deal less.

These tensions, anomalies and misalignments cause market distortions and generate unfair competition. These, in turn, can be a source of risk or harm to children and young people.

In the longer run it will not be possible to achieve the widely supported objective of building sustainable confidence in the internet as a medium for commerce, or anything else for that matter, if it continues to be seen as a cause or facilitator of avoidable risk or harm to children and young people. Addressing the identified tensions, anomalies and misalignments in policy is therefore not only a worthy purpose in its own right, because it will reduce the risk of harm to children and young people, it will also help build a broader basis of trust in the internet[13].

Analysing online commerce

When looking at the online world it can sometimes be very hard to separate out in any sort of neat or easily intelligible way the interplay of a range of different laws, regulations and self-regulatory codes on the practice of advertising, marketing, sales, data collection, data usage, data privacy and safety. It gets even harder to do this when it comes to children and young people because their specific concerns or interests as minors cut across all of those areas. The issues interlock, the one shading into the other.

Nonetheless to facilitate some sort of contained analysis CHIS below suggests a possible line of demarcation, though it is undoubtedly imperfect and could be improved upon:

1. The "free internet"

   Services such as social networking sites, search engines and location aware applications typically are provided at no cost to the end user at the point of use but they are still nonetheless highly commercial in nature. One of the principal challenges which arises in the context of these sites and services concerns the capacity of a child or young person to give informed consent to some or all of the data collection processes and data uses that are associated with or are ancillary to how the sites or services operate.

Many of the free sites and services which operate in the UK specify age limits e.g. the age at which you can become a member or the age at which you can use the service, but it is far from clear what the status or legal significance of some of these age stipulations might be if they were ever to be tested in a court within the UK.

2. The "pay as you go internet".

   Here issues arise in respect of the online sale of goods and services which are legally restricted according to the age of the person wishing to buy them. In these cases the question of the child's or young person's capacity to consent does not arise. No one can consent to purchasing goods or services illegally or to aiding and abetting such purchases.

The economic dimension

A report commissioned by Google and published in October, 2010, "The Connected Kingdom[14]", suggests that in 2009 the internet contributed £100 billion, or 7.2% of GDP, to the UK economy. This made it larger than construction, utilities, transportation and several other long established industrial sectors.

In 2009 approximately 250,000 people were employed by e-commerce companies and the report says the value of the UK's internet economy is expected to grow by 10% per annum until it reaches 10% of GDP by 2015.

The "Connected Kingdom" report discusses some of the methodological challenges the authors had to confront when assembling their data and making their findings but the burden of its principal conclusions cannot be in doubt. The internet is not only now central to many aspects of the UK's social life it is also of enormous and growing importance to our national economy.

The recent growth in online retailing provides more evidence for the latter proposition. An ever larger share of retail activity is expected to continue to shift to online environments[15]. In August 2010 UK shoppers spent £4.4 billion online, up 15% on August 2009.[16]

Moreover the level of economic activity which in one way or another is tied to children and young people is sizeable.

In 2006 children and young people in the UK up to the age of 19 spent £12 billion from their own pocket money or earnings derived from part-time jobs. When one adds to the equation the amounts spent by parents on their children, over which in varying degrees children and young people have some influence, in the same year the total value of the market increased to almost £100 billion[17]. In February 2010 it was estimated that on average it costs a family in excess of £200,000 to see each child through to their 21st birthday[18].

This loosely defined but large children's and young persons´ market is therefore of major economic significance, not just to individual firms competing for parts of it, but also for the UK's economy. The size of the market also helps explain why so many companies are interested in it.

Direct evidence of the importance attached by internet companies to children and young people as actors in the economic space emerged in a recent article in the "Wall Street Journal"[19].

Advertising – a key building block

The Journal's investigation focused on the use of "cookies", "beacons" and other tracking technologies. Typically these collect information about the web sites a person visits and the kinds of things they do when they are on them.

Your browsing habits say a lot about you and your tastes. This is precisely why

these data are so valuable and so sought after by advertisers. As the Journal observed, the data can cover

> age, tastes, hobbies, shopping habits, race, likelihood to post comments and general location, such as city.

It is because of tracking technologies, or in some cases information derived directly or expressly from the individual, for example in their profile or through their postings, that when they go online and fire up a web browser or sign in to the service they straight away find ads served up to them which mirror their recent online activity and wider interests. This practice has become known as "online behavioural advertising", usually shortened to "OBA".

The justification for OBA is eminently reasonable. It is meant to ensure that an individual is not plagued with advertisements for things they are not interested in and would never buy.

To the extent that such practices help reinforce people's existing patterns of behaviour there could be a downside to OBA, but the upside is also very clear. The problem with OBA lies in its perceived intrusiveness, its reliance on data which is all about you as evidenced by what you do when you go online. That is why the question of informed consent is so important and why the ability to decline any involvement with OBA is also vital.

The companies collecting the data which is used in OBA maintain that they separate them from anything that would allow an individual internet user to be traced or identified by any process of reverse engineering but that view does not go uncontested[20] and anyway it is not entirely or the whole point.

Companies such as Google and Facebook collect these data and retain them. They do not sell them on or provide them to any third parties. The data form the basis of their offer to advertisers. Other companies collect the data and sell them. The Journal discovered one list available for sale to advertisers going under the soubriquet "Teeny Boppers".

Children's web sites and data

The Journal's investigation revealed that

> popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults

The article looked at 50 sites that were popular with American "teens and children". Media giant Viacom owned eight of the 50 sites. The sites in question were all associated with Nickleodeon TV, a channel aimed squarely at younger children. They also looked at 50 of the most popular US sites which were principally aimed at adults.

The children's sites had placed 4,123 tracking devices on to the computers which had accessed them. This was 30% more than were found on the adults' sites. Google seems to be the single most active company in relation to placing tracking tools on sites principally used by children.

A specific example cited in the Journal article concerned a 10 year old child who reported that Google consistently presented her with ads for "pets… 'virtual worlds' and 'online goodies' such as little animated graphics to decorate a website".

Many companies say they make no attempt to collect data which is *solely* about or of interest to children, moreover the constraints imposed by the rules about advertising to children still apply, or ought to[21]. Accepting in good faith that in the above illustration Google did not knowingly target the child, did not engage in intentional behavioural advertising

aimed at children or did not deliberately collect data which was only likely to be of interest to a child, it has to be said that they might as well have done. The end result was the same.

The fact that companies go to such lengths to obtain the kind of data discussed here from web sites most commonly frequented by children and young people is very telling. It shows beyond any shadow of a doubt that children and young people are economic targets on the internet, just as they are in the real world.

The UK's Internet Advertising Bureau (IAB) rules[22], prescribe 13 as the minimum age for which "segments" of OBA can be created. It is not entirely clear whether or how this aligns with rules issued by the Advertising Standards Authority (ASA) and the Direct Marketing Association (DMA) where 12 is given as the minimum age at which information can be collected without prior parental approval.

In research carried out for the Office of Fair Trading[23], "Attitudes to Online Markets, Report by FDS International" (FDS Report)[24], at para 9.16 it is revealed that 37% of the sample were either "very concerned" or "somewhat concerned" about cookies. That is a big number. If the same survey question was asked again but it was preceded by an explanation of how cookies work in relation to children and young people it must at least be a possibility that the percentage would come out even higher.

It is true that it is always possible to block cookies and beacons or to get rid of them[25], and the IAB rules, for instance, expressly say that adherents to their code must provide a

> clear and unambiguous notice to users that it collects data for the purposes of OBA. This notice shall include information about what types of data are collected, how these data are being used and how users can decline OBA…

However, companies that use these technologies vary enormously in the effectiveness, amount of time, energy and resources they devote to ensuring their customers, users, or web site visitors are fully briefed in the way the IAB rules clearly intend. Not everyone makes it equally easy to avoid OBA.

Cookies and similar tools predate OBA by many years and they are not only used as a means of supplying data that ends up in an advertiser's database. There is no doubt that cookies can be very useful and save internet users a great deal of time, but some companies appear to be taking unfair advantage of that fact. They seem to rely on consumer exhaustion or perplexed frustration to get their customers, users or web site visitors to set their browsers always to accept cookies or to opt for the default settings, or just to click "yes". The default settings or the "yes" click typically are calculated to maximise or at any rate to enhance the company's revenues. Using complexity and fatigue to bamboozle consumers is common in many markets but it is inexcusable in all of them.

Children are economic targets

As we have seen, children and young people plainly are economic actors and economic targets on the internet, as they are in the offline world. This ought to be explicitly recognized and incorporated into future policy making, both generally but also specifically in relation to policy around tracking technologies and the advertising and data collection practices which they facilitate.

Children and young people are of course entitled to participate in economic activity, online and off. Indeed they need to do so

as part of the process of growing up, learning how to handle money, and anyway within reason it can be a lot of fun. However, many of the rules and practices which have been established to protect children and young people from unfair commercial practices in the real world e.g. about encouraging excessive or inappropriate spending and "pester power" do not yet seem to have been fully translated into the virtual space or to have found an online equivalent or proxy.

Given the meteoric rise of OBA[26] it may no longer be satisfactory or make sense to divorce the question of advertising from the data collection processes on which an already substantial and still growing proportion of it is based, particularly in the case of children and young people. In any event not all of the current codes and rules which appear to be or claim to be relevant in this space are wholly in sync with each other[27].

A definition and a method of determining what constitutes a children's or young person's web site or other area of online activity which is specific to or targeted at children and young people may need to be agreed and established as a standard which all regulators and self-regulators could integrate into their codes.

Consideration may also need to be given to developing particular rules for advertising and other practices on "mixed" locations i.e. sites or areas where children and young people are in a minority but where it can be shown they are nonetheless present in substantial volumes.

For example, should children's and young people's web sites, or sites used by large numbers of children and young people, be encouraged to develop a system of easily understood icons to indicate, explain and overlay the site's fuller data collection and data usage polices?[28]

A growing number of virtual worlds aimed exclusively at very young children now exist. One of the largest is "Club Penguin". When Disney acquired the business in 2007 they were reported to have paid US$700 million for it, again underlining the highly commercial nature and magnitude of the economic interest in children's and young people's activity in the online space[29].

Many virtual worlds seem to rely for their income stream on a combination of monthly subscriptions and the sale or promotion of branded virtual and real merchandised and other products.

The promotion of these products could be via "advertorials", normally text or pictorial representations which are not always easily distinguished from advertisements.

"Advergames" are another method used to sell things. These are games which might, for example, be won more easily or rapidly if the child buys[30] one or more of the weapons or tools on offer.

Alternatively a child is prompted to buy virtual furniture or decorations to improve the appearance of their personal site, as was the case with the 10-year old referred to above in the Wall Street Journal article.

Are these types of situations adequately accounted for and covered in the existing codes of the principal bodies with an interest? Does the speed and immediacy of the internet change anything or call for new thinking in terms of how children and young people now buy things?

Most of the existing rules designed to protect children and young people in the

commercial field were drawn up in and for an analogue world where slower processes were common. The gap between seeing something you think you want and being able to get it has been potentially hugely truncated by the internet. The emergence of "one click purchasing" compresses it even further.

Impulse buying is often a curse in the adult world. Do we need to do more to protect children from it in the online space?

Sending a faulty product back that arrived in a box in the post or was bought at a shop on the High Street is one thing. How easy is it for a child or young person to return or get a refund for a virtual product they have paid for and downloaded? Are they made aware of their rights in this regard and how sympathetically, swiftly and simply do companies honour those rights? Is a nine year old expected to grapple with Customer Services?

In many situations where children and young people are buying things online a parent will necessarily be involved to supply the household credit card, but this is by no means a universal rule. The banks, financial institutions and sites themselves have come up with several new ways of putting online purchasing power directly into the hands of minors[31].

Regulatory concerns

The UK's Office of the Information Commissioner, the Commission of the European Union, national Governments both in Europe and elsewhere, the Article 29 Working Party[32], as well as regulators from other areas or disciplines continue to express concerns about the use of tracking technology and other aspects of online data collection and usage. They do so both generally but also specifically in relation to the way it may be impacting on children and young people. Technological convergence seems to be generating its own regulatory convergence as the interdependence of the different strands of activity becomes clearer.

Specifically in the field of advertising and marketing in the UK the ASA, the DMA as well as the IAB have all recently been seeking to address some of the issues discussed here but it is still far too early to say whether or not they have succeeded in allaying all of the concerns that have been expressed. At the time of writing some of the provisions of the freshly revised codes are not yet operative. In fact it is not clear that important elements in the world of online advertising and marketing regard some aspects of the revised codes as being entirely settled and accepted[33].

Chapter 2 Market distortions and unfair competition – the "pay as you go internet"

Online sales

Having established that 18 is *a* key point of departure in commerce, it is not the only one. Over the years laws have been passed and regulations have been promulgated to restrict the sale of a number of goods and services to persons of various ages below that of 18. Online these laws appear to be honoured more in the breach than in the observance.

Appendix 1 contains a list of the different goods and services to which a legally-defined age limit applies.

The list of items that are age restricted and the ages applied to them are identical in all four nations that make up the UK, except that for Scotland a few extra items would need to be added to have a complete list.

Age restricted goods and services

A major part of this submission addresses concerns about the sale over the internet of age restricted goods and services.

Appendix 1 shows that there are around 20 such items. It is acknowledged that there is room for more than one view as to whether or not in every single case the right age levels have been chosen but that is a different argument. The UK is very unlikely to abandon the idea of having legally defined age restrictions of any kind for all or most of the items currently on the list or to proclaim that it has given up on seeking to enforce them, either online or off. Thus even if new age limits were set, for a larger or smaller set of commodities or services, issues of compliance or non-compliance in the online space would continue to arise.

A journey to adulthood

Children and young people are on a journey towards adulthood. Their bodies may not be suited to the consumption of certain products e.g. alcohol, or it is thought they lack the necessary judgment to be able to handle a range of items safely e.g. larger knives. Alternatively legislators have taken a view that some activities e.g. gambling should only be available to adults, or they have decided that particular types of material e.g. pornographic videos or violent computer games should only be sold to adults.

Young people down the ages have always sought to challenge conventions and test boundaries. Risk-taking, rebelling against or seeking to manipulate "the rules" is in varying degrees a perfectly normal part of the process of growing up[34]. The fact that

the rules are sometimes broken, or it is difficult to make them work always wholly as intended, is no reason for abandoning them altogether, or for giving up on the attempt to enforce them when necessary.

Rules, particularly rules backed up by laws, are a reflection of societal norms and values. They shape and influence behaviour and expectations, even in the breach. Equally the absence of rules implies permission, endorsement, consent or acquiescence of some kind.

In the case of age restricted goods and services available online the internet provides an easy way of evading the legally required visual age checks that are standard on the High Street. With the notable exception of the gambling industry, referred to in more detail below[35], it appears that the great majority of online retailers, active in many different markets, make no serious efforts to determine the actual age of any persons attempting to buy age restricted products or services from them. This means they are regularly breaking the law and they must or ought to know it. Their acts of omission are putting children at risk.

Examples of compliance failures

Persons below the age of 18 are not allowed to buy knives which might be used as an offensive weapon. In practice this is generally taken to cover any knife with a blade longer than three inches. In July 2009 trading standards officers in the London Boroughs of Lambeth and Southwark published the results of a survey they had carried out into the sale of knives online. A summary of their findings is attached as Appendix 2. The survey revealed that whereas in previous tests carried out on the High Street 19% of attempts by minors to buy knives illegally succeeded, online 93% of attempts made by minors were successful.

Under the terms of the original research that was carried out neither Southwark nor Lambeth would disclose the names of the companies that had supplied the knives to under age persons but it is understood that several household names were implicated.

The London Borough of Greenwich trading standards officers carried out a similar examination of under age sales made online. They covered a broader range of products, but they also included knives. Greenwich gave no undertakings about not disclosing the names of the companies that had provided goods to persons not legally qualified to buy them. The results of their study were published in May 2009 and are provided in Appendix 3. Several very well-known companies are named as law breakers e.g. Marks & Spencer, Argos, Amazon and Oddbins. Most of these also have High Street stores but it is seriously doubted that there would have been anything like the same "success rate" in relation to under age persons obtaining similar items from them in their bricks and mortar establishments.

There are other examples which could be produced following similar investigations into online retailers carried out by trading standards officers in Cardiff, Salford and Staffordshire. These show that this problem exists across the UK, not only within London.

Nonetheless CHIS makes no claims that it has evidence of large scale law-breaking in relation to the online sale of age restricted goods and services but then CHIS knows of no one who has undertaken any large scale research into the matter. The few systematic studies that have been published have been carried out by overstretched trading standards officers. Almost by definition such studies are going to be small scale and very local in nature but every time anyone looks a similar picture emerges. Things are not

getting better. As online retailing grows, unless countervailing measures are taken, the situation is only likely to deteriorate.

It will be observed that in the press statements made by the London Boroughs[36] there were some companies that did manage to prevent illegal sales from happening online, and as we shall see later in this report the gambling industry has achieved a very substantial degree of success. If some companies can do it, why is it not possible for all of them to do it?

The Daily Mail picked up on the story about the illegal sale of knives online. In their edition of 1st July, 2009[37], James Roper, Chief Executive of the Interactive Media in Retailing Group (IMRG),a leading e-retail industry body, is quoted:

> We take the important issue of age-restricted sales online very seriously indeed.
>
> We have formed an 'Age Verification Online' working party to collectively address the issue in order to protect the rights of consumers to legitimately purchase products and services.
>
> We are working towards creating an industry standard so that both online retailers and customers can be assured that we're doing everything possible to ensure that age-restricted products are sold responsibly.

At the time of writing there is no news of a final outcome from this working party but through correspondence it is clear they are seized of the importance of the issue.

In the same edition of the Daily Mail a spokesperson for the British Retail Consortium (BRC) is quoted as follows

> Our members are totally committed to using their experience of successfully preventing under 18s buying alcohol to stopping them buying knives.

In the immediate aftermath of the story appearing a number of larger companies announced that they were going to stop selling knives online altogether[38]. The BRC has an internal working party, the Distance Selling Policy Action Group, actively considering these issues across the full spectrum of age restricted products and services. The results of the group's deliberations are awaited with great interest. CHIS will be responding to a recent invitation to contribute to its work.

Could get worse for the High Street

It seems likely that as the volume of online retailing continues to grow across the board High Street and smaller retailers are bound to come under increasing economic pressure. Inter alia this is likely to make them ever more watchful of online competitors' trading practices, particularly if there is any suggestion that they are competing against them unfairly or in ways which discriminate against them unreasonably.

More and more High Street stores are adopting a policy whereby, if a person looks like they may be under 21 or under 25, they are being asked to produce proof of age. Some of these young adults may well decide to buy age restricted items online rather than suffer the potential embarrassment or inconvenience of having to produce proof of age at the checkout.

Online firms are unlikely to adopt a similar self-denying ordinance. Indeed there would be no reason for them to do so since they cannot see their customers anyway, but this again reminds policy-makers about the evident lack of a level playing field as between the real and virtual worlds.

Either way the more efficiently the laws on age restrictions are enforced on the High

Street, the greater is the likelihood there will be a drift towards online sales for such items and the greater will be the legitimate outcry from law-abiding High Street vendors if they see their position being further undermined by unfair means.

For some vendors that operate both offline and online a shift from High Street sales to online sales may be a matter of little immediate or urgent concern from a purely business perspective. To the extent that online trading is more profitable than High Street trading it may even produce an increase in their turnover and an increase in profitability. However, for those stores who are confined solely to the High Street or who have little or no online presence, the sense of grievance will be that much more substantial and justified.

In informal conversations with some major online retailers they do not dispute their legal obligations are. In essence what their "defence" comes down to is something like this

> OK. We accept there is an issue but you are making a fuss over nothing or very little. The penalties are tiny. The effort of putting this problem right is disproportionate, too expensive. It's just not worth our while. I guess if we started to get a lot of stick over it in the press or the fines increased we would have to act but in the absence of that we probably won't, or anyway not any time soon. The banks should sort this out. Not us.

Such frankness is commendable at one level. It makes clear what the nature of the challenge is. Legal compliance is an optional extra, fines at the moment are an almost insignificant business expense which can be written off.

"Proportionality", like beauty, is in the eye of the beholder. It all depends where your priorities lie.

Compliance success – gambling

The challenge of underage gambling has been around for very many years. In a recent survey 2% of adolescents – 60,000 12-15 year olds – were classified as "problem gamblers"[39].

Starting in about 2002 a number of CHIS members began to receive phone calls from parents about their children developing problematic gambling habits through online gambling web sites.

Children were going online, ticking a box to claim they were over 18 then using their own legitimately acquired debit cards to spend all of their pocket money on the horses. In a small number of cases it was clear that some had become addicted and were engaging in theft or deception to sustain their addiction.

In 2004 the children's charity NCH[40] initiated a piece of research. It did this working closely with Citizencard[41] and GamCare[42].

NCH targeted 37 UK focused gambling web sites. It first wrote to each of them asking if they were satisfied with the arrangements they had put in place to detect and deter under age persons from using their site. Irrespective of their replies, two months later, each site was visited. 30 of the sites were unable to detect a 16 year old coming to their site to gamble. She simply ticked a box to affirm she was 18 and got through.

Enforcement was weak

In the case of gambling, then as now, there was no doubt about the law. Under 18s were not and still are not allowed to gamble[43]. All the gambling companies spoken to in the course of NCH's research

said they were aware of the problem of children improperly using their web sites and lying about their age. They all said they were "very concerned" about it.

Nothing happened. The authorities had the necessary powers to act but it was clear that understaffing among enforcement officials, uncertainty about jurisdictional issues and the scale of non-compliance meant that, in effect, no one felt capable of ensuring the law was being observed.

No more complaints

The Government and Parliament decided to intervene. They did this via the Gambling Act, 2005. This made installing a robust online age verification system a condition of obtaining a license to operate a gambling web site[44]. Several new companies sprang up in order to provide the technology and the service to enable online age verification to take place.

The idea is very simple: to gamble online a person must first open an account. To do that the individual enters their personal details on to an online form. The gambling site makes clear that because it is supplying an age restricted service it must check and confirm that the applicant is 18 or above.

In effect the gambling site asks your permission to carry out checks[45]. In practice what this means is that the site sends the would-be gambler's information to an intermediary where it is checked against any of several online databases to which they have access. The largest of these are those held by credit reference agencies. If all the data matches and confirms the age is 18+ then the process is complete and the individual is able to gamble. The process can be completed in a matter of seconds and the cost is carried by the site.

It is understood that approximately 95% of all adults in the UK are on one or other of the online databases to which the intermediaries have access. For the 5% who are not[46], or for those who object to being verified in this way, alternative paper-based systems are available although, obviously, these will take a little time to complete. The person will not be able to gamble online straight away.

The age verification processes and associated procedures which the Gambling Act, 2005 ushered in do not appear to have had any negative effects either on the overall profitability or the performance of gambling companies.

Since the regulations came into effect in September 2007, the children's charities are not aware of a single instance where the rules have been breached by a child[47].

It is true that no system is ever going to be entirely foolproof but the example of gambling appears to show that some can work to a very high level of efficiency.

If such systems are good enough for gambling they ought to be good enough for alcohol, knives and any other products that have a legally-defined 18+ label or which proclaim they are only suitable for persons aged 18 or above.

What is noteworthy about the gambling case study is that the great majority of the gambling firms only moved when they were all forced to do so. The 2005 Act meant no one could gain an advantage by refusing to do it or by delaying unduly. Self-regulation did not produce the goods. It is a lesson that is not lost on others.

Verifying sub-18s

From the example of the gambling industry we can see that where a product is

limited to adults, systems already exist which appear to be working satisfactorily.

The same cannot be said in relation to the position of sub-18s. To develop a scalable system for verifying the ages of persons below the age of majority is acknowledged to be a substantial undertaking.

The current climate is not the most propitious for discussing initiatives of this type. Because of spectacular disasters and misjudgements elsewhere[48] a major backlash against "the database state" is underway and even though there is no suggestion that such a project ought necessarily to be undertaken by Government the auguries are still less than ideal. Yet a trustworthy scheme owned and managed by someone or by some combination of partners is essential if the UK's age related laws are to continue to have any relevance in the internet age.

The first and major challenge is to devise a means of obtaining reliable, verifiable data on children's and young people's ages which can form the basis of whatever technology is applied to its deployment over the internet.

What has been lacking up until now is any obvious determination on the part of major online retailers or the financial institutions, or both, to resolve the problem of how to originate, authenticate and keep secure the primary or initial data. Each sector seems to think it is the other's responsibility. In reality they have a shared responsibility. The Government should consider pressing for a joint initiative to take this forward within an acceptable timeframe. There are several possibilities.

A system which mirrors that used for issuing passports or the real world "PASS" cards[49] would be one way of gathering in the data[50].

Alternatively schools could be enlisted to the cause. Every child attending a school in the UK is given a log in of some kind when they enrol. This enables them to use their school's computers and access the internet. Would it take much extra effort to extend that into a secure system which could also be used externally?

The banks are one of the most obvious potential sources of a solution. When a child, or indeed anyone, opens an account with them they go to considerable lengths, as required by the anti-money laundering rules, to establish the true personal attributes and identity of the would-be account holder.

By whatever means the initial data is collected the relevant part of it e.g. the bit confirming the person's age, then needs to be converted into a form where it can be rendered to online vendors. Again there is more than one way in which this could be achieved.

One method could be for the verified person to be given a "digital token" of some kind, probably based on a form of public key encryption or incorporated into a dongle, or both. This digital token or the data on the dongle would be provided to any web site selling an age restricted product or service. By asking for and receiving this type of proof at the point of sale the vendor would discharge their legal obligation to take reasonable steps to check the would-be buyer's age.

Arguably such a system could provide a higher level of personal security or privacy for individuals, particularly where the product or service is bought and consumed wholly on the internet. Instead of having to render all of their personal data to every commercial web site, such a system could allow the person to produce a token confirming they had been verified as 18 or above and the vendor would need to know no more.

Clearly no one should be compelled to have an age verified ID or they should be able to choose how they are verified. Moreover individuals can, at least for the foreseeable future, still obtain almost all age restricted goods in the real world. But failing to develop a system that can be used online for under 18s is tantamount to abandoning the laws altogether. That is not acceptable.

Real world age checks

As already noted a very obvious key difference between online and offline retailing is that in the real world it is comparatively easy to carry out on the spot visual age checks. Such checks in an online environment are not a realistic possibility for the foreseeable future. Perhaps they never will be.

Could real world checks made at the point of delivery be a substitute?

In 2009 CHIS carried out some research prior to submitting its evidence to a Home Office review of the sale of alcohol. The review had a specific section within it on remote sales[51].

It is not suggested that this research was large scale enough to be wholly representative of online retailing and some information was provided to CHIS on the basis that the companies would not be publicly identified. However, the results did marry with other evidence that is available in the public domain e.g. the investigations carried out by trading standards officers in the London Boroughs of Greenwich, Southwark and Lambeth referred to above.

In discussions with companies it emerged there were starkly contrasting views as to what the law currently required. There were broadly three views:

1. A very small number of companies said that for some products, not all, they thought they had an obligation to check online at the point of sale *and* at the point of delivery. It was not always easy to get them to provide any additional information about which products they believed fell into this category.

2. Other companies accepted they have a clear obligation to do an age check at the point of sale, whether the sale is made online or offline. Their view was that in the online space the check needs to determine that the person buying the goods, the one whose card is being used to pay, is over the age of 18.

   However, according to this view, once the online age verification of the card owner has been carried out, neither the vendor nor its agents e.g. the delivery company, had any further obligations to do any kind of age checks on anyone when the goods are delivered.

   It was acknowledged that, in a remote environment such as the internet, there was no way of being sure that the person using the card on the web site to make the purchase was in fact its real owner. A parent or other adult might knowingly lend a child their credit or debit card. If the child does not already have it, the adult may also give them any additional information that is necessary to complete the sale e.g. details of the address where the card is registered. For all practical purposes it is impossible to detect this sort of behaviour, but it also raises different issues. It is not a reason for refusing to do anything.

3. A third group of companies took the view that with online sales they had no legal obligation to check the age of the purchaser at the point of sale. They insisted their *only* responsibility was to

ensure an age verification check happened at the point of delivery.

Companies that took this view accepted that the requirement to do the age verification check at the point of delivery applied whether the delivery was made directly by them or was made by agents, typically external couriers. However, there was then a further sub-division of opinion:

a) Some companies in this group thought the purpose of the age check at the point of delivery was *only* to determine that a person aged 18 or above was present when the delivery was made. That person's relationship to the person whose payment card had been used to make the purchase of the goods being delivered was thought to be immaterial.

b) Another view was that whoever made the delivery had to determine that the person whose payment card had been used was verifiably over 18 *and* was also present.

CHIS is perfectly happy for age checks to be carried out at the point of delivery, and perhaps in some cases for certain items this should be explicitly required.

However, given the immense practical difficulties or, in some cases the impossibility of doing them e.g. where the product is bought and consumed entirely online, checks at the point of delivery can never be an acceptable or complete alternative to carrying out online age checks at the point of sale.

Who delivers?

Typically once goods have been ordered online they will be delivered in one of two ways: either the vendor company will have use of or own a fleet of trucks, normally carrying their own livery using their own directly employed drivers or the delivery work will be contracted out.

FedEx, UPS, DHL, and Royal Mail

Where the delivery of age restricted goods is contracted out, for all that a number of vendors had told CHIS they accepted that a check at the point of delivery is a legal necessity, at the time of making the submission to the Home Office review in 2009 there was nothing on any of the web sites of, for example, FedEx, UPS, DHL, or the Royal Mail which indicated they had any special procedures in place.

To confirm this CHIS spoke to each company. They all said more or less the same thing:

> We have a list of prohibited items that we will not deliver at all or will not deliver without special arrangements being made… Our charges are based largely on weight, size, distance and speed. Once we have accepted the box from the customer we put it on the van then hand it over to whoever answers the door at the delivery address. We do not check the age of the person accepting delivery, neither do we check anything else about them, other than to ask their name when they sign for the goods, but actually we do not ask for any proof of that either.

What should be checked?

If a check were to be done at the point of delivery what would the check need to establish? Should it establish that the adult vouching for or taking receipt of the goods is the actual purchaser, or that he or she is another adult expressly authorised to act on the original adult purchaser's behalf?

Quite how a driver would do either of these things is another matter, but it is unlikely to be satisfactory to say that the only obligation is to determine that someone, anyone, over the age of 18 is present.

What if the person has no idea what is in the box being delivered? The driver may not know either. It may not be obvious from the external appearance of the container.

Should the person accepting delivery insist on the box first being opened so they can confirm that they are not being unwittingly dragged into a scheme to supply alcohol or some other restricted items to minors? What happens if the box is opened, the third-party sees what it is and refuses to take responsibility? Is the box then to be re-sealed and put back on the van?

Van drivers in court?

Whether the goods are delivered by a courier company or by the company's own employees, CHIS is not sure how satisfactory it is to make legal compliance in this area hang solely on the performance of the driver. What would the consequences be for the driver if it turns out an error had been made and alcohol or some other age restricted items had been handed over to a minor or to someone intent on passing them on to a minor? Would drivers start getting dragged into court as witnesses or as the accused?

Pressure to deliver

Once goods have been paid for online and are handed over to an in-house driver or a courier company all the pressure within the system is to get the goods delivered, not brought back.

The driver may well be on a bonus for finishing their round quickly or for coming back empty-handed, or both. Some may lose money or be penalised in some other way if they fail to complete their round within a given timeframe. Maybe the driver will be anxious about being parked illegally or about blocking or restricting other traffic while being compelled to park inconveniently in order to make a delivery. Entirely understandably the driver will not be keen to hang about on a doorstep while someone in the house finds a document to prove who they are or how old they are, let alone what relationship they are to the owner of the card that was used to make the purchase.

Some companies specifically allow online customers to say in advance that the goods can be left at another house, usually a neighbour's, or be secreted in a particular part of the garden. It is unclear how checks would work in these circumstances.

Trade union perspective

More particularly, and this point was made with some force by Unite, the trade union (which contains the former Transport & General Workers Union), if drivers get embroiled in age verification on the doorstep, there may be a substantial risk of them also getting involved in arguments about a person's true age or identity, and that would carry with it the risk of violence, or considerable additional stress. After all, as far the would be recipient is concerned they have already paid for the goods. The goods are theirs. They may be eagerly awaited, perhaps as a birthday present for someone. The driver is simply dropping them off, not adjudicating on their right to take delivery.

Licensed to sell age restricted goods?

No retailer is compelled to sell anything online but if they are going to choose to sell age restricted goods then they should only do so if they are in a position to demonstrate that they are doing it legally.

It is quite wrong for retailers, essentially, to take a calculated decision to delay taking action knowing that the weak nature of the enforcement regime, the trivial nature of the fines and continuing lack of media attention means they have little or nothing to fear. As online shopping grows, as it becomes easier and quicker to pay for things over the internet, if action is not taken sooner, it is likely to be harder to put it right later.

Unless online retailers show they are making a determined effort to resolve this problem within a reasonably expeditious timeframe then, as with gambling, the Government and Parliament should step in to establish a licensing regime[52].

A licence would only be given to a company that could show it had a robust online age verification system in place. There would be no need for a complicated enforcement action to be brought against offenders. The licence would be the key. Trading without one would on its own and without more constitute an offence. A hefty fine, or worse, would act as a major incentive for companies to comply.

As with gambling, when selling an age restricted product or service a company should not be allowed only to ask the person seeking to buy it to confirm their age by ticking a box on an internet page. However, having made good faith efforts to verify a person's age e.g. by using systems such as gambling companies deploy, if a company is still deceived and sells or supplies a product or service to someone below the legal age, the company should not be liable either in civil or criminal law.

Comparisons within retailing

In the preceding section specific examples were provided showing that the laws on the sale of age restricted goods and services were being observed by a small number of companies but were being broken by many more. The next sections analyze how market distortions and anomalies manifest themselves at a general or strategic level as between different types of firms competing against each other across a wide range of online and offline markets.

High Street v Cyberspace

An individual can obtain goods or services either from a bricks and mortar establishment, or remotely, now typically over the internet.

In the case of the High Street, vendors are expected to be aware of any restrictions which apply to the sale of the products on their shelves. They will also normally know at least three further things:

1. They have a responsibility to satisfy themselves that anyone attempting to buy any age restricted goods or services in their shop meets the minimum age requirement. As previously noted, they are required to do this by carrying out a visual inspection of the person making the purchase and in the event of there being any doubt they must ask for proof of age. If satisfactory proof is not forthcoming they must refuse to sell the product or provide the service.

   Any culpable failure can have severe consequences for the vendor. In the case of the sale of alcohol the sanctions can include the forfeiture of one's license, a fine, jail, or all three. In large supermarkets and other chain stores training programmes and computer systems have been put in place to allow the vendor to demonstrate that they are taking all reasonable steps to discharge their legal obligations.

2. The law and regulations apply at the point of sale, right there in the shop.

They may also apply elsewhere and there may also be consequences further up the supply chain but that is a different and an additional matter.

3. Local authority trading standards officers periodically do test purchases. Vendors always have to be on their guard. Members of the public can also observe plainly illegal behaviour and report it without difficulty.

The first and most obvious anomaly is therefore clear. Even though, as CHIS contends, the law is exactly the same for both online and offline worlds, except in the case of gambling there is no equivalent or comparable enforcement, monitoring or reporting regime in place in respect of goods and services sold online. This discriminates unfairly against shops on the High Street.

Cyberspace v Cyberspace

Similar arguments apply equally where companies are competing against each other entirely online.

Some companies have decided to ensure that when they are trading online they are complying with the law, others have not. The ones that have not may obtain a competitive advantage in two different ways:

> By failing to make the investment in developing an age verification system companies can conserve their cash. Indeed they may also be adding to it by virtue of unlawful sales. Perhaps these firms can deploy such cash in other ways that help develop their businesses, thereby putting their legally compliant competitors under further pressure.
>
> They are reducing their potential involvement in, as they see it, any off putting or time consuming processes that are a necessary part of carrying out an age check. These could put off some customers and drive them elsewhere[53]. Again law abiding firms lose business. Rogue traders gain.

These scenarios set up a situation where all the economic incentives point towards not complying with the law, when it should be the other way around.

"Brand damage" through adverse publicity has clearly not yet been sufficient to persuade many Boards of Directors that they should put these matters right. Perhaps the Directors and the journalists who cover these matters both erroneously believe there is nothing that can be done.

Domestic v Domestic

Some firms said they believed that where a company's operations are comparatively self-contained geographically, for example within a single local authority area, they are more likely to be the subject of compliance actions by trading standards officers. A local shop or local chain of shops might be an example. By contrast it has been suggested that where commercial operations are highly dispersed or decentralized, as typically they would be in the online world, it can sometimes be harder to determine the locus of the offence or offences and so compliance actions are undertaken less frequently because they are more resource intensive.

On a related point, where a vendor is a major employer within a particular local authority area there is a sense that the trading standards officers in that area will sometimes be more sympathetic to the company's position.

In one Northern city a particular company informed CHIS that their local authority trading standards officers had given them specific advice on an issue connected to online age verification. When it was put to

this company that no other trading standards officers appeared to share that view, they simply grinned and shrugged their shoulders.

The report on "Better Regulation of Age Restricted Products: A Retail View", published in August 2010 by the Local Better Regulation Office[54], suggested there was a need for aspects of the enforcement of regulations and laws in this area to be harmonized and simplified. Whilst not necessarily agreeing with all of the report's recommendations the case for this at least seems unanswerable. Curiously, this report makes almost no mention of the online aspects of the sale of age restricted goods and services. Correspondence with authors of the report has shed no light on the reasons why that was the case.

Physical v Virtual Goods

Most of the comments made up to this point are only of relevance where what is at issue is the sale of physical goods which are going to be delivered to a specific real world address. There are, however, a range of goods and services which can be bought and consumed entirely online. The most obvious examples are downloadable age restricted games or streamed videos. In these cases the only practical way of age verifying has to be online[55].

Domestic v International

CHIS encountered a view among some UK-based online vendors which suggests they appear to believe they are at a disadvantage selling age restricted goods or services when compared with other online vendors operating from foreign jurisdictions where, they believe, regulation is either a great deal lighter or non-existent.

Cross border shopping online is still comparatively unusual and UK residents are among those least likely to buy physical goods from anywhere outside the UK[56]. Price advantages can quickly be eroded by additional transportation costs and if the item originates outside the EU it might also attract levies or duties. But even so it is simply not the case that the UK is the only country which has or tries to enforce regulations about different kinds of online sales.

However, there does appear to be some real confusion or uncertainty about UK retailers' responsibilities to verify the age of persons placing orders from abroad for age restricted items, particularly where the item is to be delivered to an address outside the UK. What if the product is either not age restricted in the purchaser's country or the age restriction is lower than it is in the UK? Does the online retailer have any kind of obligation to find out about and apply the law applicable in the buyer's country or the country where the item is to be delivered if that is not the same?

Similarly what does the law say about a UK resident buying an age restricted product on the internet from outside of the United Kingdom, either from a jurisdiction where there is no age restriction at all or from one where the restriction is lower than that which prevails in the UK?

Added complexity

In relation to the online sale of goods and services the situation in the UK has undeniably been complicated by the emergence of pre-paid cards, gift cards and other forms of stored value cards.[57]

The emergence of pre-paid cards

Gift cards can be tied to particular shops e.g. Debenhams, or to a specific online provider e.g. eBay or MoshiMonsters, a children's virtual world. CHIS is currently unaware of any issues in relation to them. They seem to be set up to work within fairly well defined and narrow parameters.

There was a time when it was widely, if wrongly, thought that if an online vendor insisted on payment with a credit card this was the same as saying they would only deal with persons aged 18 or above.

Today this position is no longer tenable. A plethora of cards using the Mastercard, Visa, Maestro, Amex and other payments networks have become available. Some are sold and promoted for use "by persons of any age". Others seem to specify 13 as the minimum age at which the cards can be used.

Much to the annoyance of the companies promoting them, the link to and use of the Visa and Mastercard logos means these bits of plastic are destined to be known for quite some time as "pre-paid credit cards".

Pre-paid credit cards are on sale in corner shops, petrol stations and many other retail outlets, large and small. Whilst some say they should only be sold to persons over the age of 18, as we have noted that is not the case with all of them and anyway there is no law requiring this. Enforcement of that provision is thought to be, for all practical purposes, non-existent.

FSA regulatory oversight does not extend to some of the cards in question because they are promoted by financial institutions based overseas. Alternatively even where the FSA's writ would otherwise run, full "Customer Due Diligence" measures do not need to be applied to the pre-paid credit cards described above. This is because they form part of a class of "non-re-loadable e-money" products and the maximum amount that can be spent using such cards is set at the comparatively low level of €150, although there is a proposal to increase the amount, possibly very substantially[58].

Where the product is a re-loadable pre-paid card or the amount involved is larger, there seems to be less scope for misrepresenting the person's age because it appears the transaction has to be tied to an existing bank account or credit card or to involve some other level of identification. It is only the non-reloadable low value cards that in practice have few if any constraints or checks.

The non-reloadable cards can, in effect, be bought and used anonymously[59] and, as already noted, where the product or service being bought online is downloadable or is wholly consumed online there is not even the possibility of a secondary check at the point of delivery.

To some observers the upper cash limits of these cards may seem comparatively small, but for many purposes, including many criminal purposes e.g. buying child abuse images, counterfeit software, alcohol, tobacco and knives the limits are quite substantial. It is important also to remember that more than one card can be bought and used at the same time or in combination.

Pre-paid cards featured in the London trading standards investigations referred to earlier. Debit cards were also used and these likewise can present a challenge in relation to facilitating under age sales. Debit cards are now routinely issued to children as young as 11 by some of the High Street banks as well as other financial institutions. However, with a debit card the possibility of anonymous use does not arise so it is thought they are unlikely to feature regularly in many types of criminal activity.

People will find it a little odd that financial products or services, particularly financial products or services sporting household names such as Visa and Mastercard, can

be sold in the UK yet not be the subject of direct regulation or control by the FSA simply because the companies promoting them are based outside of the EU.

Seemingly it will soon be possible to make it a requirement for all e money products from outside the EU to conform broadly to internal EU standards. A consultation is currently under way in this area[60].

It is sincerely to be hoped that if any new rules emerge they will close down the possibility of using pre-paid credit cards anonymously on the internet or other remote environments.

Facilitating low value payments in the real world is one thing, rather like Oyster cards in London or Octopus cards in Hong Kong, but if the authorities blindly allow these technologies to translate into the online space they will, in effect, be opening the door to a potentially enormous increase in low value, low level crime. Law enforcement agencies will not thank them for this, and neither will anyone else.

Visa, Mastercard and the other card franchises are doing a lot to try to stamp out the improper use of their online payments facilities generally, but the fact that they have allowed these new types of pre-paid cards to emerge in the way that they have does rather run in the opposite direction and begs several questions.

Some of the pre-paid card issuers have taken steps to block their use on certain types of web sites e.g. sites which are specific to particular age restricted products or services such as gambling or alcohol, but not all of them have done this and many age restricted items are on sale through generic sites e.g. supermarket websites, where it seems such restrictions cannot be applied so easily.

The banks and financial institutions quite properly point out that, where the sale of an age restricted product or service arises, under the current law it is the retailer's responsibility to determine the age of the person doing the buying, in the online world as it is in the real world. There is no doubt that is true but one cannot help but feel some sympathy for the retailers as the financial institutions promoting these prepaid cards have certainly not made their job easier in respect of online sales.

It should not be possible for any method of payment to be used online to facilitate an illegal purchase of an age related product or service, but those pre-paid cards which can be bought for cash and used without any effective form of authentication of the user, seem almost to have been customised to facilitate illegal trade of one kind or another. It is the anonymity that opens the door to that.

The advantages of pre-paid cards are plain enough in terms of reaching out to the large number of people who cannot gain access to conventional credit or who do not want it for whatever reason. CHIS has no locus or reason to object to the cards on principle. But the problems they have created need not have been and they ought to be addressed, either by their creators (the finance industry) or their business benefactors (retailers) or both.

Even if the banks or financial institutions which ultimately stand behind these cards were to agree to give them serial numbers or unique identifiers which would allow all online retailers to identify the cards as they appeared in an online purchasing process, where would that leave the retailer?

Retailers could either refuse to accept such cards as methods of payment for anything, not a very likely or useful outcome, or they could refuse to accept them as payment solely for any age restricted item. In the

latter case the retailers would still be left with the task of having to code all of their age related merchandise in such a way that it could be identified at some stage during the transaction process.

If an age restricted item or service was being bought on its own, or if the web site sold only those items, it might be relatively simple to deal with it. If the age restricted item was being bought as one item among many others that were not age restricted, it becomes that bit more complicated.

On their web site the BRC say

> One challenge facing retailers that sell age restricted products is the increased prevalence of pre-paid credit cards. Currently there is no way of identifying the age of the owner of one of these cards. We believe Government should ensure that the card industry provides a way for retailers to be able to identify pre-paid credit cards so they can then exclude them from being able to make purchases of age restricted products.[61]

CHIS entirely understands the BRC's point of view. However, as we have seen, merely being able to identify pre-paid cards is not the only thing that matters.

Strictly-speaking the retailers do not need to wait for the banks to do anything, at least to deal with items that are limited to people aged 18 or above. Admittedly it seems unfair that the banks should not contribute in some way to a solution but if an independent age verification system were in place, such as is used in gambling, the link between the method of payment and the proof of age would be separated.

This scenario would also greatly expand the number of ways companies could transact with individuals for the sale of age restricted products or services. A visit to major gambling web sites will today reveal that they are capable of taking punters' money in all the usual ways e.g. via Visa, Mastercard, Maestro, but also via several more obscure or exotic channels e.g. "U Kash", "Neteller", "Western Union", "Click and Buy", and "Moneybookers".

In terms of making progress on solving this problem, there seems to be an element of "buck-passing" between the retail and financial services industries. Insiders speculate that this is partly to do with concerns on the part of the financial industry both about potential liabilities which could arise from them having any part to play in authentication processes which are primarily intended to benefit third parties and about who would bear the cost of developing a system. On the other hand the retail industry appears to feel they should not have to bear the cost of "putting right" the banks' and other institutions' original thoughtlessness.

The truth is that whereas the retailers have a clear legal requirement to act, the banks and financial institutions have an equally clear moral obligation to play a full part in resolving this problem.

The present stalemate is unhelpful. A joint initiative should be developed but for this to occur it requires some large players to decide that they want it to happen.

Chapter 3 Market distortions and unfair competition – the "free internet"

Data collection and advertising

Online advertising is a key driver and means of financing major parts of the internet. This is especially the case in relation to those web based services which are provided at no cost at the point of use.

The sustained growth of online behavioural advertising suggests that a significant and still growing proportion of *all* online advertising is linked to online data collection about individuals. One "informal" estimate[62] suggests that in 2009 80% of all online advertising campaigns "involved tracking of some sort". As one industry commentator put it[63]

> The advertising business, in short, loves online tracking just about as much as privacy advocates hate it.

Informed consent given freely and deliberately is essential to almost all data collection and data usage processes. But no one can give valid informed consent if they do not know about or understand key elements of the proposition being put.

This whole topic therefore raises areas of legal uncertainty in relation to the capacity of children and young people to give such consent. By the same token there are questions about the legal capacity of commercial concerns to solicit or otherwise obtain, store or process personal data from or about minors.

Complexity as a weapon

Issues similar to those raised earlier in relation to cookies and tracking technologies also arise where more overt or direct forms of data collection or data usage controls arise e.g. on social networking sites where your declared interests or even your online conversations and postings can be analysed and fed into an algorithm that produces information that advertisers build on.

A computer screen is not a natural or easy medium for grappling with lengthy and sometimes highly technical legal language. The screen of a typical mobile device is even less suited to this task.

The complexity of multiple control settings, frequently located in obscure parts of the site, spread across different sections or buried within applications, rarely helps children or young people or their parents to understand the nature of the proposition. Bamboozled or fatigued consumers are unlikely to be properly engaged or informed. Thus there are continuing suspicions that many online companies are failing to discharge properly their obligations to obtain

informed consent both in relation to adults and in relation to children and young people where the burden is heavier.

There is a very evident tension built into the relationship from the start. On the one hand many web sites collecting data about individuals have an interest in persuading or enticing people to reveal as much information about themselves as possible, to enrich their data set and hence its value to advertisers. On the other hand, in relation to children, young people and other vulnerable groups that may lack the knowledge, understanding or the competence to make appropriate decisions about matters of this kind, the dangers of disclosing too much information shade into areas of risk, not just of commercial exploitation but also to their physical or mental well-being.

The emergence of some new applications e.g. location based services is likely to generate new levels of anxiety. Addressing these issues is becoming urgent, particularly for children and young people[64].

The Facebook generation

The principal form of commercial online services provided free at the point of use that are of major relevance to children and young people are those clustered around social networking sites, of which Facebook is the prime example. However, there are many others e.g. music sites such as Spotify and then there are the search engines that everyone uses of which Google is by far the most dominant.

Much of the media coverage of child safety issues and social networking focuses on the way in which children and young people expose too much personal information about themselves, leaving themselves open to bullying or ridicule, or have accepted too many people as "friends" whom, in reality, they do not know at all. Addressing these sorts of questions specifically is somewhat outside the scope of a paper of this type but they most certainly do intersect at different points with concerns about how informed consent is obtained to join a social networking site, how informed consent is obtained to make use of a specific service or how it is obtained prior to the first use of a search engine. Various guides appear from time to time, some of which are truly excellent[65] but one is bound to wonder about online services which profess themselves to be easy and transparent to use only to see a whole new branch of publishing opening up to explain just that.

The problem of data collection

Earlier CHIS commented on questions of data collection and informed consent in relation to tracking technologies. These questions arise on both the "pay as you go" and the "free internet" but on the free sites there are additional questions which are peculiar to them.

It is accepted that the larger social networking and other sites and services do not knowingly advertise, market or promote age inappropriate items to children and young people, neither do they deliberately target advertisements at children and young people[66]. However, since none of the sites seek to verify the declared ages of their users there is a disjuncture here which perhaps ought to be considered in terms of it being an unfair trading practice.

For example if High Street companies carefully ensure they only advertise adult oriented products or services in media or places which are restricted to or are normally only used by adults, this being anyway a requirement of the ASA and other regulators[67] yet their online competitors regularly advertise on internet

sites which fail to observe or are incapable of observing the same or similar rules, the whole purpose and value of the real world rules are undermined or eroded. It is also very obviously unfair and discriminatory.

Following some egregious examples of inappropriate advertising and data collection practices aimed at or affecting children[68], as previously noted, the ASA and the DMA have both recently taken a series of steps to reshape advertising and marketing policies to try to ensure that contemporary practice in their respective areas of concern meet current legal, ethical and other expectations[69].

CHIS very much welcomes the changes that the ASA and DMA have made. Perhaps this will help kick start a wider discussion about age and the internet because, otherwise, the changes may well turn out to be based on a chimera.

If sites do not know, and in effect refuse to know, the real ages of their users then in what sense can they be said to be seriously concerned about ensuring that age inappropriate advertisements are never served up to children and young people or that they are properly obtaining informed consent from children and young people in relation to the associated data collection practices in which they engage?

Many social networking and similar free sites decided that young people in the UK can become users only if they are aged 13 or above[70]. There is no legal basis for this in UK law. It is simply a reflection of a US Federal law[71] designed to deal with advertising aimed at children. More than 10 years after that US law was drafted and in the context of Web 2.0, advertising remains key but it is not by any means the only point at issue.

The same US Federal law bestows legal immunity on sites for any potential breach of the age rules providing only that the company does not have actual knowledge that a person is under 13. Again there is no UK or European equivalence for such a blanket immunity or safe harbour. This US law has had a chilling effect on innovation. It means the sites have no legal incentive at all to establish whether or not a given individual is under the age of 13. On the contrary they have every reason not to find out.

Nonetheless it is true that sites say they will expel anyone they find to have misrepresented their age and some claim to have systems which can detect such misrepresentations by deploying clever algorithms. But whatever the sites are doing it is very obviously not working well enough for some of them.

Free sites know, or ought to know, that they have very large numbers of children and young people as users who have misrepresented their age solely to gain access or become users[72].

In the UK OFCOM has shown that 20% of all persons aged between 8 and 12 are users of one or other social networking site which specifies 13 as its minimum age. In certain categories this rises to 25% of all persons aged between 8 and 12. In the USA studies have shown even higher levels of underage usage.[73]

Even if these sites were to raise their minimum age level to 30 it would make no difference at all if they still refuse to verify or are incapable of verifying the age of anyone joining them.

There is an argument which says that social networking sites should abandon all age limits or make clear that their limits are purely advisory. Indeed some smaller sites have never had age limits. There have also been suggestions that the big sites e.g. Facebook, should create specific areas for

pre-teens. These are all interesting ideas which CHIS would happily discuss further but certainly in the Anglophone countries CHIS can see no immediate prospect of the current situation changing. Thus for the time being the debate will be constrained by and take place within the context of existing laws and practice.

A major debate took place in the USA in 2008-9 in which 49 States' Attorneys General banded together to try to get large social networking sites to introduce age verification for all users.

Because there was no commercial transaction involved in joining the site in the first place there were immense practical difficulties associated with this idea. However, many of the Attorneys had promoted the concept primarily as a way of ensuring that the sites would be able to keep out sexually predatory adults who might prey on children. A distinguished panel of experts, ably assisted by the University of Harvard[74], showed how age verification could never guarantee such an outcome and the proposal has since withered on the vine.

CHIS agreed with the experts' and Harvard's view. Age verification has a very narrow, specific role and value in the online space. It ought not to be over-burdened with expectations it can never hope to fulfil.

Is "free" too high a price to pay?

In the end the so-called free services are almost invariably supported by advertising which, in turn, depends on actual sales being made somewhere along the line. The use of the word "free" is therefore in some sense deceptive.

"Free" creates, or tries to create, the impression that there is at some level a philanthropic or altruistic mission underpinning the service being provided. Perhaps there was at an early point in a given company's history but, as the annual sales revenues and market capitalization of some of the enterprises concerned demonstrate, that long since ceased to be the case. These firms are very successful businesses. They have simply found another way of bringing in the revenues.

However, there is another point of wider significance tied up in this notion of "free". The companies that provide so-called free services consistently promote the view that precisely because their services are free they are entitled to be judged by standards which differ from those that are applied to companies which obtain their revenues in other ways e.g. through collecting a monthly or other subscription or through the direct sales of products or services.

In the first adjudication following her investigation of Facebook, the Canadian Privacy Commissioner, Jennifer Stoddart, acknowledged

> We have accepted that a certain amount of advertising is something users have to agree to since use of the site is free and the company needs to generate revenue.

However, the Commissioner went on to say that the issue of consent still remains[75].

Undoubtedly some latitude ought to be allowed for services which continue to be made available free at the point of use, but the reality is the currency being used is not cash but something else. It is personal information i.e. information about people's tastes and interests that is likely to be of value to advertisers[76].

Should companies that operate over the internet and utilise the free model be required to spell out more clearly the commercial nature of their exploitation of

the data rendered to them? This would certainly help those sites which genuinely are philanthropic or altruistic and who make absolutely no commercial or other use of a person's data. What limits should there be to the latitude allowed to sites which are free at the point of use?

As previously noted, data protection commissioners around the world have started to rein in some of the companies, notably Facebook and Google, that have exploited the free model where issues around privacy and consent to use personal data have arisen[77]. Might it now be timely for economic regulators, with their responsibility for examining the operation of markets from the perspective of the wider public interest, to join or collaborate more fully with data protection and privacy regulators? Many of the issues are simply different sides of the same converged public interest coin.

The original predictions about commerce on the internet were that it would let "a thousand flowers bloom" i.e. each and every internet user would become a potential internet entrepreneur who would be in an identical position to everyone else vis-à-vis every potential market or customer. In the early days of the internet examples were cited of people making surf boards in Cornwall and selling them online to people living in Australia. In fact the internet's "network effect" appears to have accelerated trends towards monopoly.

A comparatively small number of companies now dominate several important markets, not just in their own home territories but also globally. Google and Facebook are perhaps the best known examples in their respective spaces. Microsoft's wider dominance of the software market has been reinforced by the free provision of Internet Explorer. Google and Facebook in particular have achieved their degree of market dominance by using the free model as their "selling point".

Many of the companies that exploit the free model correctly point out that nobody compels anyone to use their services. However, in truth their businesses have established new societal paradigms. It may be going too far to say that Google is now almost the equivalent of a public utility in some countries, but there are hints of that about it.

Spiderman and apparently also Socrates[78] both observed that

> With great power comes great responsibility

In the modern world, companies that exercise great power and fail to demonstrate a continuing commitment to using it responsibly and fairly will inevitably set themselves on a collision course with Governments. It may be a long time coming, but it will come.

As some companies' market dominance has grown it has become entirely unrealistic to speak of anyone having a choice about accepting their terms of service, much less seek to amend them. Neither can you stand aside from the services they offer, haughtily or otherwise.

In some schools the network effect operates to make it more or less impossible, or at any rate very difficult, for any child or young person *not* to be on the same social networking site as everyone else. It is not so very different for many small or medium-sized businesses and private individuals.

Rather the questions are now about how these very large companies ossify, how they exploit their market dominance, perhaps including in ways which inhibit new competitors from entering the field.

The same companies point out that they would not have succeeded in the first place if they were not in some way or another meeting a real and proven need. This is also true, but only up to a point.

For one thing "the first place" could now be a very long time ago. Secondly it is ridiculous to suggest the internet giants are passive in this process. They do not simply respond to signals from the market, although of course they do that as well. Through their own inventiveness, their own marketing and advertising, their own investment decisions, they can establish new products and shape the expectations and norms which develop around them.

Moreover if a company with, say, 600 million users worldwide finds that everything is working well for 575 million of its customers it will probably think it is doing a great job and not feel under any great pressure to address the needs of the minority of 25 million who may be losing out or who may be putting themselves at risk in some way by using their service.

In addition, because it is very likely that the 25 million are spread all over the world, it is possible that in many countries the numbers will not be large enough to attract a sufficient head of steam to claim the attention of national Governments or local regulators. Only the company has access to the data about what is happening on their network. There is no global regulator or world governance body to whom they could be said to be accountable. No one outside the company need ever find out anything, or at least not for a long time. Yet it is very likely that within that notional 25 million will be persons drawn from any of several potentially vulnerable groups.

More added complexity

With social networking and other free sites and services no payment is required to gain admittance or access. As a result it is not possible to look at the question of children's and young people's use of free sites in the same way as one can where the sale of an age restricted product or service is at issue. The child or young person is not buying anything as such. Yet with social networking and other free sites unquestionably children and young people are moving into commercial environments.

In the UK a child acquires data privacy and data protection rights literally at birth. Those rights are personal to that child and strictly-speaking can only be exercised by the child's parent or guardian up to the point where the child is judged to be competent to do so on their own behalf. There is no law which defines a minimum or specific age when a child can lawfully act on his or her own behalf in terms of providing personal information about themselves to third parties without reference to their parents or guardians.

Information Commissioner's Office

In the "Data Protection Guide" issued by the Information Commissioner's Office (ICO) it simply says

> Consent must…be appropriate to the age and capacity of the individual and to the particular circumstances of the case.

In the "Personal Information online code of practice" the ICO develops the point[79]

> **Age and understanding**
>
> Assessing understanding, rather than merely determining age, is the key to ensuring that personal data about children is collected and used fairly. Some form of parental consent would normally be required before collecting personal data from children under 12. You

will need to look at the appropriate form for obtaining consent based on any risk posed to the child. You may even decide to obtain parental consent for children aged over 12 where there is greater risk. This has to be determined on a case by case basis.

The ICO has broadly stated what has long been considered to be best practice in the world of child protection and child welfare i.e. that determining the child's actual level of understanding in any given situation is the key test. It is a subjective test which should be applied case by case, child by child. However:

i) By referring to the age of 12 in the way it appears in the text the ICO has, not intentionally but in effect established 12 as the UK's minimum age at which children and young people can render data to third parties without first obtaining parental consent. "Spotify" uses 12 as its minimum age in the UK.

In the new ASA and DMA Codes 12 is given as the minimum age for the collection of data without "first obtaining the consent of the child's parent or guardian". However, as noted above within the IAB code 13 is specified as the minimum age for which online behavioural advertising is considered appropriate[80].

The collection of data and advertising are not wholly co-terminus but it looks a little odd that a company seemingly could collect data from 12 year olds without parental permission but cannot then target advertising towards the same data subjects until they are a year older. Are the companies collecting data from 12 year olds taking special steps to ensure that it never falls into the hands, perhaps, of departments even within their own companies that engage in OBA?

ii) The ICO is offering a counsel of perfection. It is of no practical help at all on the internet. CHIS is not aware of a single company or organization of any kind anywhere in the world where, over the internet, subjective assessments are routinely made of an individual's capacity to understand the nature of a transaction being put to them as a prelude to determining whether or not to engage with that person or provide them with a product or service.

Other countries

As is apparent from a recently issued research paper and consultation document, "The State of the Electronic Identity Market: technologies, stakeholders infrastructure, services and policies", at EU level there is a very obvious determination to see the market in e identification develop across the EU27[81].

The Commission sees it as the key which will unlock further expansion of e commerce, especially cross border e commerce. The paper does not dwell on the issue of age verification but it is referred to in several of the country analyses which are published within the document. It would be very surprising if age verification did not feature in whatever might emerge from the processes that the Commission has set in train.

From the Commission's paper and from another published by the Spanish Data Protection Agency[82] it is clear that a

number of countries have developed large scale systems which are or can be used to verify age online e.g. Germany and Belgium although quite how these feature in e commerce contexts is not always clear.

In Spain[83] and the USA[84] legislatures have passed laws which establish a much clearer position in important respects.

The Spanish law expressly addresses the age at which a child can give information about themselves to a third party. Concomitantly it also establishes for companies a baseline which they must respect. In Spain that age is 14.

The American law was originally motivated by a desire to protect children from advertising but in the end it was more widely drawn[85].

The US's COPPA law specifies 13 as the age at which a young person can render information about themselves without first obtaining verifiable parental consent. Whatever its original intention this law seems to have been interpreted in the same way as the ICO's advice in the UK has been in relation to the age of 12. Both are now widely seen in their respective countries as establishing a general safety as well as a data privacy threshold. These ages have, willy nilly, become woven into the wider debates about children's and young people's online lives. They have assumed a general significance which was never intended and is not supported by any specific evidence, one way or the other.

But it is more complicated even than that. If a young person is told he or she is old enough to decide what information to give about themselves to third parties, without referring to their parents, if they are told in effect they do not actually need their parents' engagement to open an account, then there is an implicit assumption or message being broadcast that they are also competent to deal with any and all of the issues they are likely to confront in the environment they are about to go into. For the overwhelming majority that is doubtless true but it will not be true for all young people and the dynamic it sets up is potentially problematic.

If a young person of 13 has the right to join a site without parental consent or approval then where exactly does that leave the parent? These rules can set up tensions within families so it is important to know that they are the best and the right rules, expressed in the most helpful way.

CHIS very firmly believes that young people do have a right to privacy and to a growing degree of personal autonomy as their knowledge and competence develops, usually with age. That is not what is at issue. Rather it is about how the debate is constructed, and later de-constructed.

A new "gold standard"?

Blunt and crude though it may be, in relation to the internet CHIS can see no alternative but to follow the example of the USA and Spain.

A minimum age should be specified and given the force of law in the UK. Above this age, in the absence of any specific information indicating there is a potential issue, companies would not be obliged routinely to seek prior permission from parents before collecting or storing data from young persons. Below that age they always would.

Consideration should also be given to establishing this age as a new, generic online safety threshold which should translate across the whole online and digital space in the UK. It could become an age "gold standard".

The alternative, having a multiplicity of standards applying at different ages, or no age, will create loopholes through which

many will jump as confusion follows. Exactly what the age gold standard should be ought to be the subject of consultation and fresh research[86]. It may turn out to be somewhere around 12 – 14. On the other hand, as previously noted, in the context of some practices the ASA has chosen 16 and the DMA has even designated 18[87].

There is no suggestion that changing the law for the purposes of the internet or other remote environments need have any impact at all or require any alteration to the current law applicable in any situation where the child is visible to and in the presence of the vendor of a product or would be provider of a service. In those instances the existing laws and rules would still apply.

Either way, in matters such as these companies need clarity and consistency. The current state of the law in the UK is anything but that in relation to the internet.

However, notwithstanding any decision that might be taken about the appropriate minimum age at which children and young people can act on their own behalf in data transactions of different kinds, without a means of verifying their age online the outcome may not change much in practice.

Perhaps if in the UK the problem could first be solved in relation to the sale of age restricted goods and services, where there is an existing legal driver, a solution might evolve, paid for by commercial concerns, which could be adapted or used in other settings.

Obviously, as with all things to do with the internet, the more an age standard could be internationalized the more likely it is to find favour with internet companies, but the difficulties associated with doing that in this area are likely to be substantial and ought not to be the basis for unduly delaying taking any action in the UK.

Chapter 4 Conclusions

Cumulative effects

It seems likely that, unless corrective measures are taken, the negative effects of the tensions, anomalies and misalignments of policy which have been highlighted in this report will increase over time, further distorting markets or further promoting unfair competition, while continuing to put children and young people at risk.

Regulation and the internet

One of the internet's oft' revered greatest strengths, its lack of any single point of management or control[88], is also the source of one of its greatest weaknesses.

When "bad things" happen on the internet it can be incredibly difficult to get the key players together to agree how to respond, even within the Anglophone countries, let alone on a wider basis. Fear of such a meeting being construed as a cartel at work explains part of it, but probably not all of it.

It is often a useful shorthand but there really is no single "internet industry" anyway. There are firms which provide access to the internet but in reality there are now many companies across several industries that use or own bits of the internet. Some of the internet's largest and best known companies have little or no investment in its basic infrastructure.

Even if a small number of large companies were to agree to do something, the way the development and propagation of new applications works on most platforms means that there really are currently no mechanisms for guaranteeing anyone else will take any notice.

Those who worry about anti-competitive practices, those for whom preserving the freedom to innovate appears to be an end in itself, take great comfort from this, but sadly this situation leaves it open to others to jump in and suggest their own remedies.

Usually these "others" are Governments. As a result of Government pressure in many different countries we are already seeing the beginnings of the fragmentation of the internet. This process will continue, it may even pick up speed, unless the interested parties come up with a formula that will make Government interventions unnecessary or at any rate will minimise the potential of such interventions to do any lasting harm to the fundamental idea of an open, global network. That entails finding a way to make it clear that self-regulation can work. Simply saying "trust us we're the internet industry" is not a viable option.

In a recent landmark study of "The Impact of the Commercial World on Children's Wellbeing", Professor David Buckingham and his associates found that

> New media and marketing techniques raise some ethical concerns about potential deception and threats to privacy: the public is not currently well-informed about this area, and existing regulation is insufficient in some respects.[89]

This is a view CHIS shares.

Elements of the internet industry have assiduously promoted the idea that it is very difficult to regulate the internet and that because of its highly devolved nature there is little that can be done. If that was ever true is open to doubt, but it is far from being the case today.

A person living in the UK who hears of a new product announcement in, say, the USA or Japan may find they are not able to order it over the internet. Typically the vendor's servers will detect the person's IP address, realise immediately that they are physically located outside the territorial borders of the USA or Japan and automatically put a block on completing the transaction.

Alternatively, in the case of certain physical goods, this will happen when the person provides details of where the product is to be delivered or the buyer provides details of the currency in which they want to pay. The internet can be borderless, but only if you want it to be.

As the internet began to take off in the consumer space in the mid to late 1990s few Governments or regulators really wanted to jump in with strict or close regulation at least in part because they feared choking off local growth in the new world economy that was rapidly opening up. Fewer still felt confident enough to challenge the powerful, rich companies and their highly technically literate spokespeople and lobbyists who were marketing the internet as a democratic agent of liberation, a symbol of modernity, an endless source of fun and games, culture, knowledge, even wisdom. The internet was the ultimate in "cool". Doubters and critical questioners were dismissed or marginalized as fuddy duddy Luddites or spoilsports who "just didn't get it".

Today many aspects of how the internet works are more settled, even if innovation around the edges continues apace.

Certainly there are now lots more people, particularly in the public policy space, who can disentangle the hype from the reality, who understand or know enough about the technology and are more ready to query the claims and the business practices of internet companies, just as they would do any other industrial or commercial sector.

Up until now, around most of the developed world the notion of self-regulation of the internet has been the dominant idea. The advantages of self-regulation are obvious enough[90] but what matters most to CHIS is obtaining the right result for children and young people, rather than the mechanics of how that result is obtained.

In relation to many of the issues discussed in this paper, up until now self-regulation has manifestly failed to deliver. For these reasons CHIS commends to the UK Government the range of proposals made in this report. The principal ones have been brought together and summarized in the section headed "Policy Proposals" in the last part of the Executive Summary.

In particular CHIS would like to draw attention to the need for further research but perhaps more than anything there is a need for key institutions to engage.

The Government should bring together or initiate a discussion with all of the relevant stakeholders and regulators with an interest in online commerce and its associated practices to focus specifically on the position of children and young people in relation to online commerce. The UK Council for Child Internet Safety could play an important part in drawing together the different strands.

The stakeholders are likely to include the OFT, the Office of the Information Commissioner, Financial Services Authority, Advertising Standards Authority, the Advertising Association, Direct Marketing Association, Internet Advertising Bureau, Interactive Media in Retailing Group, British Retail Consortium, Trading Standards Institute, Association of Payments and Clearance Services, appropriate Government Departments, relevant academics and children's organizations.

It is also likely to be useful to involve appropriate EU institutions at an early stage as a prelude to evolving a wider strategy for engaging with a range of commercial and regulatory interests some of which are likely to be based or have their head offices in countries outside of the EU 27. Given that the EU has recently announced its intention to develop a "Comprehensive Approach on Personal Data Protection"[91] this may be an ideal moment to engage in a closer dialogue. The Commission's draft says

> children deserve specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data

The draft also speaks about the Commission potentially

> introducing specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children.

A new legal obligation?

Following her major investigation into Facebook, the Canadian Data Privacy Commissioner expressed the hope that

> …in the future, more due diligence in the area of privacy will be done by global technology firms.[92]

That is a view CHIS endorses and would like to develop.

Commissioner Stoddart's comments in Canada were directed at Facebook but they seem already to have found an echo with Google in Washington DC. On 27th October, 2010, the US Federal Trade Commission issued a statement referring to the protracted privacy dispute which had arisen with Google around the way it collected data for "StreetView". In the FTC statement it said:

> Google has recently announced improvements to its internal processes to address some of the (privacy) concerns raised, including appointing a director of privacy for engineering and product management; adding core privacy training for key employees; and incorporating a formal privacy review process into the design phases of new initiatives.

It is earnestly to be hoped that one of the first items the new privacy person at Google will look at is "Latitude" and the whole issue of location services, particularly as they are likely to impact on children and young people.

CHIS takes the view that every company that operates over the internet should be under an all-embracing explicit legal obligation to carry out due diligence in respect of online child safety. It might be called a "child safety audit" which has to be completed prior to the launch of any new product or service which they propose to release on to the internet particularly, but not exclusively, where it is proposed to supply it free to the end user. This is

because, from experience, it is known that, at least for now, on the "free internet" there is a high probability that children and young people will be able to access and use the product. There are currently potentially only very weak to non-existent audit trails to act as a brake on misuse.

An appropriate agency should be given a power to call in and inspect these child safety audits either on their own volition or following a complaint.

There is no suggestion that the product or service cannot be released until it has "passed" a Government approved child safety test but establishing a rule of this kind would force companies to think more carefully. It mirrors commonly accepted obligations to perform a range of safety checks and other evaluations prior to launching new products in the offline world.

In particular it should not be possible for any company to launch a new service or product and walk away from, avoid or reduce any potential liability by the trivial expedient of cutting and pasting a notice saying "This service is only available to persons over the age of 13" or "This service is only available to persons over the age of 18" if they know perfectly well they will make no serious attempt to police or enforce, or are incapable of effectively policing or enforcing such an age related rule. Some companies appear to make serious attempts, but few are required to do so which means most do not. That is no longer acceptable.

---ooo---

Endnotes

[1]18 is also the legal definition used in the UN Convention on the Rights of the Child, which is the cornerstone of international law in these matters.

[2]Age of Legal Capacity (Scotland) Act 1991 http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1991/cukpga_19910050_en_1. This allows, inter alia, for agreements made by 16 and 17 year olds to be set aside if they are "prejudicial transactions".

[3]See "Manifesto for a Networked Nation", http://raceonline2012.org/manifesto/1

[4]http://ec.europa.eu/information_society/activities/sip/surveys/quantitative/index_en.htm

[5]"Benefits of home access to technology", Kate Blewett, BECTa, October, 2009; A research study into the social effects of lack of internet access on socially disadvantaged children and families, 'Ofcom: Children and the internet (2007)' is available at Ofcom's website www.ofcomconsumerpanel.org.uk/information/documents; A research project, 'Digital Inclusion: A Discussion of the Evidence Base (July 2007)' undertaken by FreshMinds for UK online centres www.ukonlinecentres.co.uk/downloads

[6] http://www.homeaccess.org.uk/

[7]Scotland, Wales and Northern Ireland closely monitored the roll out and impact of this policy and are considering how it might be adopted in their education systems.

[8]For children with special needs

[9] The social aspect was also always key. Children and young people without internet connections at home are easily identified and stigmatised in the playground as "the poor kids" or the "weird kids". They are effectively excluded from a significant part of the social life of the school because they are not able conveniently or easily to make use of or engage with the social networking and other online services that almost everyone else is using in the evenings and at weekends.

[10]The population of children and young people between the ages of 4 and 17 in mid-2009 was approximately 10 million. As such they constituted over 16% of the entire population of the UK. The numbers of persons aged 65 or above was about the same but only a proportion of those are likely to be classed as "vulnerable" within the commonly understood meaning of the word. http://www.statistics.gov.uk/statbase/Product.asp?vlnk=15106

[11] These are also reasons for not taking too seriously the idea that contemporary concerns about children's and young people's use of the internet will eventually disappear as the current generation of youngsters become parents. The argument runs that today's internet users will *all* be so aware of how the internet works they will *all* be able to provide a much greater level of support to their children as that future generation, in turn, starts to become internet users. Doubtless this will be true for some of today's parents of the future, perhaps many. It is unlikely to be true for everyone and no one can know how the proportions will split. Technology changes but more importantly what is at issue here is not always or necessarily how much technical knowledge or internet experience a parent has, but what insights that parent has into their own or other people's children's and young people's uses of the technology and also how good they are, as a parent, at communicating those insights in a useful and productive way.

[12] http://www.lse.ac.uk/collections/children-go-online/UKCGO_Final_report.pdf

[13] In "Attitudes to Online Markets, Report by FDS International" page 30, section 4, it discusses attitudes and barriers to internet usage. Only 1% of non-users referred to fears about security and 7% to "not feeling confident". 8% is significant when viewed in a national context, but of equal interest are the internet users who do engage in e-commerce. Table 5.1 shows very high levels of concerns about internet security, cons, and viruses and similar. This suggests a degree of fragility in terms of a commitment to continuing to use the internet for e-commerce. The table also reminds us that, perhaps because of force of circumstances, a person can be a regular participant in e-commerce but nevertheless be a nervy or grudging one. This can also hold back the development of e-commerce. Finally there are some things which, for practical purposes, can now only be done on the internet e.g. booking low

cost flights and holidays. A person might do that and nothing else. Good news for the travel industry but it does not necessarily betoken any wide growth in or engagement with e-commerce.

[14] http://www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf

[15] http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf

[16] IMRG/CapGemini Sales Index, September 2010, see http://www.imrg.org/8025741F0065E9B8/(httpPages)/FAE5B4EDA9020E448025744F0038D60B?OpenDocument

[17] "Consumer Kids", Ed Mayo & Agnes Nairn, Constable & Robinson Ltd, London 2009, at pages 5 and 18.

[18] http://www.guardian.co.uk/news/datablog/2010/feb/23/cost-raising-child#data

[19] http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html

[20] See "Myths and Fallacies of "Personally Identifiable Information", Narayanan and Shmatikov, June, 2010, http://unescoprivadesa.urv.cat/media/_pdf/shmat_cacm10.pdf

[21] Owners of web sites visited by children and young people also point out that many of the trackers being used are installed on children's and young people's computers by third parties, not directly by themselves, implying they have little or no responsibility for them and not all trackers collect or provide information that would be of interest to advertisers.

[22] http://www.youronlinechoices.com/wp-content/uploads/2010/07/IAB-UK-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf at section 3.

[23] http://www.oft.gov.uk/OFTwork/consultations/closed-awaiting/eprotection/

[24] http://www.oft.gov.uk/shared_oft/consultations/eprotection/oft1253

[25] Although see the discussion on the emergence of so-called "persistent cookies".

[26] See below, page 30

[27] Compare the age limits used in the IAB, ASA and DMA codes.

[28] A project investigating this approach is underway in Holland led by the Netherlands Organization for Applied Scientific Research.

[29] http://www.virtualworldsnews.com/2007/08/disney-acquires.html

[30] The child might have stored value or credits on their account or have won some virtual money from the site owner.

[31] See for example the discussion of pre-paid cards and gift cards below at page 26.

[32] http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

[33] At the beginning of October, 2010, the IAB issued a draft code saying that cookies should automatically expire after 48 hours where a visitor to a web site had not actually made a purchase. The code was itself withdrawn within 48 hours. http://www.theregister.co.uk/2010/10/04/iab_cookie_advice/

[34] The Byron Review, 2008, page 20, para 1.21

[35] At page 18

[36] See Appendices 2 & 3

[37] http://www.dailymail.co.uk/news/article-1196763/One-retailers-80-online-outlets-caught-selling-knives-children.html

[38] This was an understandable response, but it was nonetheless a knee-jerk. Some people e.g. persons with mobility problems or who live in remote areas, have come to depend upon the

internet as a means of obtaining various goods and services and having them delivered to their door. If proper age verification systems were in place it would not have been necessary to stop selling these items online.

[39]"Beating the Odds", Gamcare, September 2010

[40]Recently renamed "Action for Children"

[41]Citizencard provides an age verification product

[42]Gamcare is a charity which helps individuals with problematic gambling behaviour such as addiction.

[43]With the exception of the National Lottery where the age is 16.

[44] The operation of the anti-money laundering rules also plays into the same space, reinforcing the need for gambling companies to carry out identity checks.

[45]A copy of William Hill's policy statement is included as Appendix 4

[46]These are likely to be people who have just moved to the UK or persons with no credit history.

[47] CHIS is aware of cases where children have "borrowed" a parent's credit card and created gambling accounts on which they have then spent their parent's money, but in these instances they have in effect been presenting themselves as their parent, and there is little or nothing any legislation can ever do about that. This is an example of a parent's carelessness or wilfulness allowing their identity to be abused or in effect aiding and abetting a crime. However, since the Gambling Act, 2005, what seems to have completely vanished from online gambling is the simple ruse of creating a false ID with a false age simply in order to get into a position where a child can place a bet.

[48] The cost and operational efficacy of the previous UK Government's plans to introduce a national identity card scheme was questioned by many. In trying to make the case for the scheme Ministers were not infrequently tripped up by other, non-related events. Perhaps the best known was the loss by the Inland Revenue of CDs that it put in the internal post. These contained information on 25 million British taxpayers. They never reached their destination and have never been found. It emerged in the subsequent enquiry that this was not a unique incident.

[49] http://www.brc.org.uk/pass/default.asp

[50]Indeed some companies already do this.

[51]http://www.chis.org.uk/2009/08/15/evidence-to-home-office-review-on-the-sale-of-alcohol

[52] In early 2010 Baroness Massey piloted a Private Member's Bill on online age verification through the House of Lords. It passed with all-Party support but in the end failed for want of time in the House of Commons.

[53] In fact some systems can complete the checks in about two seconds, or less.

[54]http://www.lbro.org.uk/docs/age-restricted-products-report.pdf

[55] Although an alternative would be to require people to call in at the shop first or some other real world environment to complete an authentication process which could later be used online.

[56]http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/980&format=HTML&aged=0&language=EN&guiLanguage=en

[57]There are also other forms of remote payment mechanisms available which could be exploited to facilitate illegal under age sales e.g. reverse SMS, but a discussion of them is outside the scope of this paper.

[58] In practice many of the non-reloadable cards in the UK appear to adopt an upper limit of £50 but the Treasury is currently consulting on a proposal which would raise the legally allowable amount either to 250 or 500 Euros. See http://www.hm-treasury.gov.uk/8439.htm, footnote 2.

[59] The fact that many outlets selling the cards deploy CCTV hardly counts as a complete rebuttable.

[60] http://www.hm-treasury.gov.uk/8439.htm.

[61]http://www.brc.org.uk/policymaster04.asp?id=541&sPolicy=DISTANCE+SELLING

[62]

http://www.iab.net/media/file/News_Media_Workshop_-_Comment_Project_No.P091200.pdf

[63] http://mashable.com/2010/11/03/behavior-tracking-privacy/

[64] New apps which can pinpoint an individual's physical location are starting to emerge. Location is an aspect of behaviour and therefore will present new advertising and other opportunities to companies minded to exploit them. Typically the location apps work with mobile phones and these are extensively used by children and young people.

[65] See Larry Magid's and Ann Collier's stellar offering about Facebook at http://www.connectsafely.org/fbparents. Whilst possibly the best this is by no means the only guide to Facebook. Shall we look forward to a guide to the guides to Facebook?.

[66]But see the research published by the Wall Street Journal, reported above on page 10.

[67]For example those administered by Phonepay+

[68] "Fair Game", report of Childnet International and the National Consumer Council, 2007, http://www.childnet-int.org/downloads/fair-game-final.pdf

[69]See http://www.bbc.co.uk/news/technology-11140676 and http://www.dma.org.uk/membership/mem-code.asp

[70]Or 12 in the UK in the case of Spotify.

[71]Children's Online Privacy Protection Act of 1998(COPPA)

[72] (2009). *European Online Safety Survey* [online]. Available: http://www.microsoft.com/
Ofcom (2009b). *UK Children's Media Literacy: 2009 Interim Report*. London: Ofcom [online]. Available: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/uk_childrensml/full_report.pdf [17 November, 2009].

Lloyd, K. and Devine, P. (2009). *The Net Generation* (Research Update No 62). Londonderry: Access Research Knowledge [online]. Available: http://www.ark.ac.uk/publications/updates/update62.pdf [28 October, 2009].
and http://safekids.com/mcafee_harris.pdf

[73]http://safekids.com/mcafee_harris.pdf

[74]http://cyber.law.harvard.edu/research/isttf

[75]Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc., page 7, para 14.http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

[76]See above WSJ article, page 10

[77]http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm#summary

[78] Thank you Google for helping me discover this.

[79]http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf
See pages 15 - 17

[80] http://www.youronlinechoices.com/wp-content/uploads/2010/07/IAB-UK-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf
see section 3 "Sensitive Segments"

[81]

http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=3739

[82] "Online Age Verification for Our Children", Jules Polonetsky, http://www.futureofprivacy.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf

[83] Spanish Data Protection Authority, Agencia Espanola de Proteccion de Datos (AEPD) Handbook;
http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1426

[84]The Children's Online Privacy Protection Act of 1998(COPPA).

[85] http://www.coppa.org/comply.htm

[86]For example in the UK the ICO has no clear explanation as to why it chose 12 in the first place. It seems to have been inherited from the former Data Protection Authority (DPA). It is thought the DPA adopted 12 as a standard based on earlier experience with "special offers" that were frequently mounted by breakfast cereal companies. These required a child to cut a coupon out of the box, fill it in and send it back in return for receiving, say, a plastic soldier or an animal. Apparently not many people ever complained or objected at the time so it was assumed 12 was probably OK. Basing policy on this leisurely model from the 1950s may not be appropriate for age of rapid mouse clicks ushered in by the internet age.

[87] http://bcap.org.uk/The-Codes/CAP-Code/CAP-Code-Item.aspx?q=CAP+Code+new_General+Sections_10+Database+practice_Rules_Children paras 10.15 and 10.16 and http://www.dma.org.uk/_attachments/resources/45_S4.pdf paras 2.17, 8.25, 19.30 and 19.31

[88] ICANN and IANA certainly have key roles in the overall management of the global internet but they are several layers removed from the kind of detailed control issues discussed in this paper.

[89]http://publications.education.gov.uk/eOrderingDownload/00669-2009DOM-EN.pdf at page 3

[90] Self-regulation has worked extremely well in the UK in relation to controlling access to known URLs containing child abuse images. According to OFCOM 98.6% of all UK domestic broadband users belong to an ISP which deploys a blocking list which has been produced by the Internet Watch Foundation.

[91]

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[92]http://www.priv.gc.ca/speech/2009/sp-d_20090827_e.cfm

Appendix 1

List of age restricted goods and services

The list given below is based on an extract from "Better Regulation of Age Restricted Products: A Retail View" a report prepared by the Business Reference Panel of the Local Better Regulation Office and published on 25th August, 2010[1].

Alcohol	18	Tobacco	18
Aerosol spray paints	16	Knives	18
Caps	16	Fireworks	18
Solvents	16	Butane gas lighter refills	18
National Lottery	16	Petrol	16
Video tapes & DVDs	12, 15 & 18	Party poppers	16
Air guns & imitation firearms	18	Pets	16
Cracker snaps	16	Crossbows	17

The report was prepared by retailers and therefore focuses on physical products on sale in their shops. For a complete picture it would be necessary to add on firearms, gambling and other items e.g. premium rate services supplied over mobile phone networks, where there is a regulatory requirement to comply with specified age limits.

Computer games can also be rated 18 but following a recent change in the law some will also be given legal limits of 12 and 15, thus bringing them into line with films sold on video tapes and DVDs

In Scotland allowing the sale, hire or use of sun beds or other electrically powered UV tanning equipment is limited to persons over the age of 18, and skin piercing is limited to persons aged 16 or above unless written permission is provided by a parent or guardian or a parent or guardian is present. In Scotland there also seems to be scope for local authorities to extend the range of products or services which may not be sold to minors. See for example the Angus Age Restricted Products code[2] which includes, for example, catapults, accessories to smoking, amyl nitrate, adult magazines, adult CDs with parental warnings.

[1] http://www.lbro.org.uk/docs/age-restricted-products-report.pdf

[2] http://www.angus.gov.uk/services/View_Service_Detail.cfm?serviceid=1398

Appendix 2

Press release

Online underage knife sales - project results released

Southwark Trading Standards is a top performer in underage sales enforcement and has been commended for its innovative Knife Charter for retailers. We now have one of the best compliance rates for underage sales of knives in the capital and were shortlisted for a Public Protection Achievement Award in the 2009 Municipal Journal Awards.

In light of these successes we joined efforts with Lambeth Trading Standards to win a bid for funding to carry out a project investigating the underage sale of knives on the internet. The project was supported by LoTSA (London Trading Standards Authorities), the Home Office and GOL (Government Office for London). The project results were released in July 2009.

Results

Out of 44 UK based online retailers tested over a three month period, 41 sold and delivered knives to our underage volunteer test purchasers - a non compliance rate of 93 percent. This contrasts sharply with the results of 829 underage test purchases carried out in shops across the capital by London trading standards authorities. These resulted in 113 sales - a non-compliance rate of 19 percent.
Although other trading standards authorities have previously attempted to purchase knives on-line using under 18s, it had never before been attempted to buy from such a wide range of online sellers throughout the country.

Key features of the project

Each attempted purchase involved a young person aged either 14 or 15 being overseen by a parent and a Trading Standards Officer.

They used prepaid cards which they had registered by submitting their true names and ages.

The transaction of selecting and ordering a knife was recorded electronically.
The young people did not misrepresent themselves during the transactions other than to check boxes confirming that they were over 18 or, if required during the order process, by stating an age which indicated they were over 18.

Methods used by the three companies who refused to sell consisted of a phone call or email requesting proof of age. In one instance this was prompted by an initial electoral register check.

In one case, even though evidence was requested, the sale proceeded even though the proof of age was not supplied.

The cards used in this project were available to anyone over the age of 13 and obtained using the applicant's true identity and age. At the outset of this project it was anticipated that many sales would not be processed because the card would flag up the age of the purchaser. This only happened in one of the 44 transactions attempted.

Report conclusions

It is particularly difficult to ensure compliance with proof-of-age laws when sales are made across the internet and face to face contact is lost.

Whilst the majority of traders had age warnings on their site, only 3 out of 44 carried out positive age checks that prevented the sale from taking place.

Appropriate age checks can be made by on-line traders for as little as 50p per transaction using readily available software.

Many of the retailers tested have stated that they were unaware that the pre-payment card used was available to under 18s and awareness needs to be raised in this area.

As it is becoming harder for young people to buy knives from retail premises they may turn to online sales as an easier option where controls are less stringent and there is a wider and more "impressive" choice.

Continuous trader advice and test purchasing at high street retailers has seen a dramatic fall in the underage sale of knives from such outlets. If online retailers adopt appropriate age checking mechanisms they could almost eliminate under age sales from taking place.

Next steps

The online retailers that made illegal sales have now all received informal warnings and advice. Further test purchases may be undertaken and if sales re-occur they could be prosecuted.

The report findings have now been passed to the Home Office with a view to working with stakeholders to tackle the issues raised.

Appendix 3

Embargoed to Friday 8 May 2009

Greenwich operation spotlights weakness in online protection for children
Lax measures by companies selling age-restricted goods online could be putting children at risk, Greenwich Council has discovered.

In a shocking revelation of the weaknesses in current protection measures, Greenwich discovered how easy it was for a 16-year-old to buy knives, adult-rated DVDs, violent computer games and alcohol.

In an operation supervised by Council trading standards officers, the 16-year-old volunteer went online and successfully purchased the following items:

- Knives from Debenhams, Amazon, Choice and Tchibo
- Age-restricted games for PS2 and PCs from HMV, Play.com and Game
- Age-restricted DVDs from Argos and Play.com
- Alcoholic drinks from Drinksdirect, M&S, Oddbins, Laithwaites

He made the purchases having bought a prepaid Splash maestro card and a MasterCard gift card from local retailers. Both cards were registered with his real date of birth and address. He then went online to buy the age-restricted goods.

Website capturing software was used to record the purchase of these age restricted products.
13 out of 16 (81%) of the online retailers in the Council's operation sold to the young person with no further checks at the point of delivery. The others made pre-delivery calls to the home and the council did not test whether an age restriction.

Only three of the online retailers asked the young volunteer to confirm his age at the time of making the online purchase – and he simply got round the system by giving false information, with no requirement to provide documentary proof of his age. Other sites merely declared that buying the goods was taken as a declaration that the person purchasing was 18 years or over.

Cllr Maureen O'Mara, Greenwich Council's cabinet member for neighbourhood services, said, "This operation seems to show the danger to which young people can be exposed on the internet. Many companies appear to be doing little or nothing to determine whether or not the people they are selling to meet the minimum age requirement."

Greenwich Council has written to all those firms who sold the restricted goods. The Council does not plan further action in relation to these offences.

ENDS

Appendix 4

William Hill's policy statement, copied from their web site.

"It is illegal for someone who is under 18 years of age to gamble.

In order to avoid unlawful betting, William Hill reserves the right to carry out checks to verify the information provided. We may undertake a search with a third party for the purpose of verifying that you are 18 or over.

Where these checks are unable to verify any customer is 18 or over, William Hill reserves the right to ask for proof of age. Customer accounts may be suspended and funds withheld until satisfactory proof of age is provided. The legal gambling age varies according to country, we advise you to carry out local research.

To prevent potential misuse if young people have access to a computer with Internet access please keep your account number, user name and password confidential.

For more detailed information on William Hill's Age Verification measures, please click here."